Math. J. Okayama Univ. **50** (2008), 85–99

IMAGINARY QUADRATIC FIELDS WHOSE EXPONENTS ARE LESS THAN OR EQUAL TO TWO

Kenichi SHIMIZU

Abstract. We give a necessary condition for an imaginary quadratic field to have exponent less than or equal to two. Further we discuss relations of this condition with other necessary conditions studied by Möller and Mollin, and conjecture that these conditions are equivalent.

1. Introduction

The purpose of this paper is to study relations of arithmetic invariants of imaginary quadratic fields whose exponents are less than or equal to two.

Given a square-free integer $d > 0$, we define D by

$$D := \begin{cases} 4d & \text{if } d \equiv 1,\ 2 \pmod 4 \\ d & \text{if } d \equiv 3 \pmod 4, \end{cases}$$

and call $-D$ the discriminant of the imaginary quadratic field $K_D = \mathbf{Q}(\sqrt{-D})$. We denote by h_D the class number of K_D, and denote by e_D the exponent of the class group of K_D that is the least positive integer n such that $\mathfrak{a}^n \sim 1$ for all ideals $\mathfrak{a}$ of K_D. We call a rational prime q a split prime of K_D if $\left(\frac{-D}{q}\right) = 1$, where $\left(\frac{\cdot}{q}\right)$ is the Kronecker symbol. Let q_D denote the least split prime.

We define $f_D(x)$ by

$$f_D(x) := \begin{cases} x^2 + d & \text{if } d \equiv 1,\ 2 \pmod 4 \\ x^2 + x + (1+d)/4 & \text{if } d \equiv 3 \pmod 4. \end{cases}$$

Further for every divisor $e < \sqrt{d}$ of d, we define $q'_D(e)$ by

$$q'_D(e) := \begin{cases} e + d/e & \text{if } d \equiv 2 \pmod 4 \\ \dfrac{e + d/e}{2} & \text{if } d \equiv 1 \pmod 4 \\ \dfrac{e + d/e}{4} & \text{if } d \equiv 3 \pmod 4, \end{cases}$$

and denote $q'_D := q'_D(e)$ if e is the largest divisor of d less than $\sqrt{d}$.

The main ingredient of this paper is to consider the condition $f_D(x) = q^2$ for a split prime q. We shall prove the following theorems.

Mathematics Subject Classification. Primary 11R11; Secondary 11R29.
Key words and phrases. imaginary quadratic field, class number, exponent, split prime.

Theorem 3.3 If $d \equiv 2 \pmod 4$ and q is any split prime, then there are no integers x such that $f_D(x) = q^2$.

Theorem 4.4 If $d \equiv 1,\ 3 \pmod 4$ and q is any split prime, then the following conditions are equivalent.
(1) $q = q'_D(e)$ for a divisor $e < \sqrt{d}$ of d.
(2) $f_D(x) = q^2$ for an integer x.

Furthermore for the least split prime q_D, we show:

Theorem 4.5 If $d \equiv 1,\ 3 \pmod 4$, then the following conditions are equivalent.
(1) $q_D = q'_D$.
(2) $f_D(x) = q_D^2$ for an integer x.

Corollary 4.9 If $d \neq 1,\ 3$ and $d \equiv 1,\ 3 \pmod 4$, then $e_D \leqq 2$ implies $f_D(x) = q_D^2$ for an integer x.

In the case that K_D has a split prime $q < \sqrt{D/3}$, we obtain the equivalent conditions for $e_D = 2$ as follows:

Theorem 5.2 If $d \equiv 1,\ 3 \pmod 4$ and K_D has a split prime $q < \sqrt{D/3}$, then the following conditions are equivalent.
(1) $e_D = 2$.
(2) For every split prime $q < \sqrt{D/3}$, there exists a divisor $e < \sqrt{d}$ of d such that $q = q'_D(e)$.
(3) For every split prime $q < \sqrt{D/3}$, there exists an integer x such that $f_D(x) = q^2$.

Now let us introduce several other invariants of K_D, which should be closely related to the condition $e_D \leqq 2$.

For every prime divisor p of d, we define $f_{D,p}(x)$ and $x_{D,p}$ by

$$f_{D,p}(x) := \begin{cases} ax^2 + p & \text{if } d \equiv 2 \pmod 4 \\ 2ax^2 + 2ax + (a+p)/2 & \text{if } d \equiv 1 \pmod 4 \\ ax^2 + ax + (a+p)/4 & \text{if } d \equiv 3 \pmod 4, \end{cases}$$

and

$$x_{D,p} := \begin{cases} p - 1 & \text{if } d \equiv 2 \pmod 4 \\ p/2 - 1 & \text{if } d \equiv 1 \pmod 4 \\ p/4 - 1/2 - p/2d & \text{if } d \equiv 3 \pmod 4, \end{cases}$$

where we set $a := d/p$. Writing $\nu(n)$ for the number of (not necessarily different) prime factors of an integer n, Ono's number p_D is the maximum of $\nu(f_D(x))$ for integers x in the interval $0 \leqq x \leqq D/4 - 1$ if $d \neq 1,\ 3$, and

$p_D = 1$ if $d = 1,\ 3$. Let t_D be the number of different prime factors of D, and R_D be

$$R_D := \begin{cases} \sqrt{D} & \text{if } d \equiv 2 \pmod 4 \\ \sqrt{D/4} & \text{if } d \equiv 1, 3 \pmod 4. \end{cases}$$

For these invariants, we pose the following conjecture:

Conjecture 1.1. *If $d \neq 1,\ 3$, then the following conditions are equivalent.*

(i) $e_D \leqq 2$.
(ii) $p_D = t_D$.
(iii) *For every prime divisor p of d, $f_{D,p}(x)$ takes only prime values for integers x in the interval $0 \leqq x \leqq x_{D,p}$.*
(iv) $q_D = q'_D$.
(v) $q_D > R_D$.

Furthermore when $d \equiv 1,\ 3 \pmod 4$, the following condition is equivalent to the above five conditions.

(vi) $f_D(x) = q_D^2$ *for an integer x.*

We here note that some relations have been known between those conditions of Conjecture 1.1. In fact, H.Möller proved (i) ⇒ (iv) and (iv) ⇒ (v) (see Theorem 2.5 and 2.6). R.A.Mollin essentially obtained results that imply (i) ⇒ (ii) and (ii) ⇒ (iii) (see Theorem 2.2 and 2.3). In this paper, we shall prove that (iv) is equivalent to (vi)(Theorem 4.5), and consequently that (i) implies (vi) and that (vi) implies (v) (Corollary 4.9 and 4.10).

In summary, we obtain the following relations:

$$\text{(i)} \Longrightarrow \text{(ii)} \Longrightarrow \text{(iii)}$$
$$\text{(i)} \Longrightarrow \text{(iv)} \iff \text{(vi)} \Longrightarrow \text{(v)}$$

At the moment of writing this paper, we cannot prove the other relations. Especially we have not established any sufficient conditions for $e_D \leqq 2$. But when $d \equiv 2 \pmod 4$, we can show the equivalence of conditions (i), (iv) and (v) (Theorem 3.4) by using the non-existence of split primes less than $\sqrt{D/3}$.

The organization of subsequent sections is as follows. In Section 2, we state the results about prime producing polynomials that was studied by Rabinowitsch, Frobenius and Mollin. Furthermore we also state Möller's result that $e_D \leqq 2$ implies $q_D = q'_D$. The case of $d \equiv 2 \pmod 4$ is considered in Section 3. We show the equivalence of conditions (i), (iv) and (v) in Conjecture 1.1. Section 4 is devoted to studying the condition $f_D(x) = q^2$ in the case of $d \equiv 1,\ 3 \pmod 4$. We give relations between the condition $f_D(x) = q^2$ and other invariants of K_D. In Section 5, we consider split primes q less than $\sqrt{D/3}$ and prove that $f_D(x) = q^2$ holds for every split

prime q if and only if $e_D = 2$ holds. Finally in Section 6, we show the properties related to the condition $q_D > R_D$. In particular under certain conjecture, we prove that $q_D > R_D$ implies $e_D \leqq 2$ if $d \equiv 1,\ 3 \pmod 4$.

2. Quick review of related studies

In 1772, L.Euler discovered that the quadratic polynomial x^2+x+41 takes only prime values for integers x in the interval $0 \leqq x \leqq 39$. Euler also noted that the quadratic polynomial x^2+x+A takes only prime values for integers x in the interval $0 \leqq x \leqq A-2$ in the cases of $A = 2,\ 3,\ 5,\ 11,\ 17,\ 41$.

In 1912, F.G.Frobenius and G.Rabinowitsch independently showed that the above fact is related to the class number of imaginary quadratic field $\mathbf{Q}(\sqrt{1-4A})$ as follows.

Theorem 2.1. (Frobenius [3] and Rabinowitsch [13]) *The following conditions are equivalent.*
(1) *The quadratic polynomial* $x^2 + x + A$ $(A \geqq 2)$ *takes only prime values for integers* x *in the interval* $0 \leqq x \leqq A-2$.
(2) *The imaginary quadratic field* $\mathbf{Q}(\sqrt{1-4A})$ *has class number one.*

Further Frobenius considered about prime producing polynomials related to imaginary quadratic fields of class number two. In 1974, M.D.Hendy [4] gave a necessary and sufficient condition for prime producing polynomials related to imaginary quadratic fields of class number two. These results have been generalized by R.A.Mollin [6]-[11] to imaginary quadratic fields whose class numbers are 2^{t_D-1}, which is equivalent to $e_D \leqq 2$. We give here the following two results.

Theorem 2.2. (cf. [11], p.110) *If* $e_D \leqq 2$, *then* $p_D = t_D$.

Theorem 2.3. (cf. [11], p.114) *If* $e_D \leqq 2$, *then for every prime divisor* p *of* d, *the quadratic polynomial* $f_{D,p}(x)$ *takes only prime values for integers* x *in the interval* $0 \leqq x \leqq x_{D,p}$.

Remark. Mollin defined the qth Euler-Rabinowitsch polynomial:

$$F_{D,q}(x) = qx^2 + (\alpha_D - 1)qx + ((\alpha_D - 1)q^2 - D)/(4q),$$

where $q \geqq 1$ is a square-free divisor of D, $\alpha_D = 1$ if $4q$ divides D and $\alpha_D = 2$ otherwise. The polynomial $F_{D,q}(x)$ is a generalization of $f_{D,p}(x)$.

Examples of Theorem 2.3.

(1) When $d = 190 = 2 \cdot 5 \cdot 19 \equiv 2 \pmod 4$, we have $h_D = 4$ and $t_D = 3$. If $p = 2$, then $a = d/p = 95$, $x_{D,p} = p - 1 = 1$ and $f_{D,p}(x) = 95x^2 + 2$ takes only prime values 2 and 97 in the interval $0 \leqq x \leqq 1$. If $p = 5$, then $a = 38$, $x_{D,p} = 4$ and $f_{D,p}(x) = 38x^2 + 5$ takes only prime values 5, 43, 157, 347 and 613 in the interval $0 \leqq x \leqq 4$. If $p = 19$, then $a = 10$, $x_{D,p} = 18$ and

$f_{D,p}(x) = 10x^2+19$ takes only prime values in the interval $0 \leqq x \leqq 18$; $10x^2+19$ =19, 29, 59, 109, 179, 269, 379, 509, 659, 829, 1019, 1229, 1459, 1709, 1979, 2269, 2579, 2909 and 3259.

(2) When $d = 177 = 3 \cdot 59 \equiv 1 \pmod 4$, we have $h_D = 4$ and $t_D = 3$. If $p = 3$, then $a = d/p = 59$, $x_{D,p} = p/2-1 = 0.5$ and $f_{D,p}(x) = 118x^2+118x+31$ takes prime value 31 at $x = 0$. If $p = 59$, then $a = 3$, $x_{D,p} = 28.5$ and $f_{D,p}(x) = 6x^2 + 6x + 31$ takes only prime values in the interval $0 \leqq x \leqq 28$; $6x^2+6x+31$ =31, 43, 67, 103, 151, 211, 283, 367, 463, 571, 691, 823, 967, 1123, 1291, 1471, 1663, 1867, 2083, 2311, 2551, 2803, 3067, 3343, 3631, 3931, 4243, 4567 and 4903.

(3) When $d = 267 = 3 \cdot 89 \equiv 3 \pmod 4$, we have $h_D = 2$ and $t_D = 2$. If $p = 3$, then $a = d/p = 89$, $x_{D,p} = p/4-1/2-p/2d = 0.24\cdots$ and $f_{D,p}(x) = 89x^2+89x+23$ takes prime value 23 at $x = 0$. If $p = 89$, then $a = 3$, $x_{D,p} = 21.58\cdots$ and $f_{D,p}(x) = 3x^2+3x+23$ takes only prime values in the interval $0 \leqq x \leqq 21$; $3x^2+3x+23$ =23, 29, 41, 59, 83, 113, 149, 191, 239, 293, 353, 419, 491, 569, 653, 743, 839, 941, 1049, 1163, 1283 and 1409.

Theorem 2.1 means that $h_D = 1$ is equivalent to $p_D = 1$. R.Sasaki [16] showed that $h_D = 2$ is equivalent to $p_D = 2$. But $h_D = 3$ is not equivalent to $p_D = 3$. In fact if $D = 4 \cdot 21$, then $h_D = 4$ and $p_D = 3$. Sasaki also proved that $p_D \leqq h_D$. Hence we get that $h_D = 3$ implies $p_D = 3$. J.Cohen and J.Sonn [2] conjectured that $h_D = 3$ is equivalent to that $p_D = 3$ and $D \equiv 3 \pmod 4$ is a prime. Further F.Sairaiji and Shimizu [15] showed that $h_D = p_D$ holds only finitely many D.

We have another result related to imaginary quadratic fields of class number one.

Theorem 2.4. (cf. S. Chowla, J. Cowles and M. Cowles [1]) *Assume that $d > 3$ is a prime and $d \equiv 3 \pmod 8$. Then $q_D = (1 + d)/4$ is equivalent to $h_D = 1$.*

In 1976, Möller generalized Theorem 2.4 to imaginary quadratic fields with the exponents $e_D \leqq 2$ as follows.

Theorem 2.5. (Möller [5]) *If $d \neq 1,\ 3$ and $e_D \leqq 2$, then $q_D = q'_D$.*

Further Möller showed the following theorem.

Theorem 2.6. (Möller [5]) *If $d \neq 1,\ 3$ and $q_D = q'_D$, then $q_D > R_D$.*

3. Properties in the case of $d \equiv 2 \pmod 4$

In this section we consider the case, $d \equiv 2 \pmod 4$. In this case, we can obtain some equivalent conditions for $e_D \leqq 2$.

Mollin showed the following result.

Theorem 3.1. (Mollin [11], p.122) *If $e_D \leqq 2$ and $d \equiv 2 \pmod 4$, then there are no split primes less than $\sqrt{D/3}$.*

Further we show results about split primes.

Theorem 3.2. *If $d \equiv 2 \pmod 4$ and q is any split prime less than $\sqrt{D/3}$, then there are no divisors $e < \sqrt{d}$ of d such that $q = q'_D(e)$.*

Proof. If $q = q'_D(e)$ for a divisor $e < \sqrt{d}$ of d, then $q = e + d/e \geqq 2\sqrt{d} = \sqrt{D} > \sqrt{D/3}$. This is a contradiction. □

Theorem 3.3. *If $d \equiv 2 \pmod 4$ and q is any split prime, then there are no integers x such that $f_D(x) = q^2$.*

Proof. If $f_D(x) = q^2$ for an integer x, then $x^2 + d = q^2$. Hence $d = q^2 - x^2 = (q + x)(q - x)$. Set $e = q - x$, then $q + x = d/e$ and $q = \dfrac{e + d/e}{2}$, which is impossible since $e + d/e$ is odd. Hence $f_D(x) \neq q^2$ for any integer x. □

Theorem 3.4. *If $d \equiv 2 \pmod 4$, then the following conditions are equivalent.*
(1) $e_D \leqq 2$.
(2) $q_D = q'_D$.
(3) $q_D > R_D$.

Proof. Theorem 2.5 means that (1) implies (2), and Theorem 2.6 means that (2) implies (3). Furthermore if $q_D > R_D = \sqrt{D}$, then $q_D > \sqrt{D/3}$. Hence all split primes are more than $\sqrt{D/3}$, so we have $e_D \leqq 2$. Thus (3) implies (1). □

4. Properties related to the condition $f_D(x) = q^2$ in the case of $d \equiv 1,\ 3 \pmod 4$

First we show the following proposition.

Proposition 4.1. *Suppose that $d \equiv 1,\ 3 \pmod 4$ and q is any split prime. If $f_D(x) = q^2$, then the integer x is in the interval $0 \leqq x < q$.*

Proof. We may assume $x \geqq 0$. Since $d > 0$, we have $f_D(x) > x^2$. Hence we get $x^2 < q^2$, so $0 \leqq x < q$. □

Further we give two lemmas.

Lemma 4.2. *Suppose $d \neq 1$. Let $e < \sqrt{d}$ be any divisor of d.*
(1) *If $d \equiv 1 \pmod 4$ and $x = \dfrac{d/e - e}{2}$, then $f_D(x) = q'_D(e)^2$.*
(2) *If $d \equiv 3 \pmod 4$ and $x = \dfrac{d/e - e - 2}{4}$, then $f_D(x) = q'_D(e)^2$.*

Proof. (1) If $x = \dfrac{d/e - e}{2}$, then $f_D(x) = \left(\dfrac{d/e - e}{2}\right)^2 + d = \left(\dfrac{e + d/e}{2}\right)^2 = q'_D(e)^2$.
(2) If $x = \dfrac{d/e - e - 2}{4}$, then $f_D(x) = x^2 + x + \dfrac{1+d}{4} = \dfrac{(2x+1)^2 + d}{4} = \dfrac{\left(\frac{d/e - e}{2}\right)^2 + d}{4} = \left(\dfrac{e + d/e}{4}\right)^2 = q'_D(e)^2$. □

Lemma 4.3. *Let q be any split prime.*
(1) *If $d \equiv 1 \pmod 4$ and $f_D(x) = q^2$, then $x = \dfrac{d/e - e}{2}$ and $q = \dfrac{e + d/e}{2} = q'_D(e)$ for a divisor $e < \sqrt{d}$ of d.*
(2) *If $d \equiv 3 \pmod 4$ and $f_D(x) = q^2$, then $x = \dfrac{d/e - e - 2}{4}$ and $q = \dfrac{e + d/e}{4} = q'_D(e)$ for a divisor $e < \sqrt{d}$ of d.*

Proof. (1) We may assume $x > 0$. If $f_D(x) = x^2 + d = q^2$, then $d = q^2 - x^2 = (q+x)(q-x)$. Set $e = q - x$, then e is a divisor of d less than $\sqrt{d}$ and $q + x = d/e$. Thus we get $x = \dfrac{d/e - e}{2}$ and $q = \dfrac{e + d/e}{2} = q'_D(e)$.
(2) We may assume $x \geqq 0$. If $f_D(x) = \dfrac{(2x+1)^2 + d}{4} = q^2$, then $d = 4q^2 - (2x+1)^2 = (2q + 2x + 1)(2q - 2x - 1)$. Set $e = 2q - 2x - 1$, then e is a divisor of d less than $\sqrt{d}$ and $2q + 2x + 1 = d/e$. Thus we get $x = \dfrac{d/e - e - 2}{4}$ and $q = \dfrac{e + d/e}{4} = q'_D(e)$. □

Using Lemmas 4.2 and 4.3, we obtain the following theorem.

Theorem 4.4. *If $d \equiv 1,\ 3 \pmod 4$ and q is any split prime, then the following conditions are equivalent.*

(1) $q = q'_D(e)$ *for a divisor* $e < \sqrt{d}$ *of* d.
(2) $f_D(x) = q^2$ *for an integer* x.

Proof. Suppose $q = q'_D(e)$. If $d \equiv 1 \pmod 4$ and $x = \dfrac{d/e - e}{2}$, then $f_D(x) = q'_D(e)^2 = q^2$ by Lemma 4.2. If $d \equiv 3 \pmod 4$ and $x = \dfrac{d/e - e - 2}{4}$, then $f_D(x) = q'_D(e)^2 = q^2$ by Lemma 4.2.

Conversely by Lemma 4.3, we immediately get that (2) implies (1). □

By Theorem 4.4, we obtain that (iv) is equivalent to (vi) in Conjecture 1.1 as follows:

Theorem 4.5. *If* $d \equiv 1,\ 3 \pmod 4$, *then the following conditions are equivalent.*
(1) $q_D = q'_D$.
(2) $f_D(x) = q_D^2$ *for an integer* x.

For the proof of Theorem 4.5 we state the following lemmas.

Lemma 4.6. (Möller [5]) *Suppose* $d \neq 1,\ 3$. *If* $e < \sqrt{d}$ *is any divisor of* d, *then* $q'_D(e)$ *is a split prime or a product of split primes.*

Lemma 4.7. *Let* e_1 *and* e_2 *be any divisors of* d *less than* $\sqrt{d}$. *Then* $e_1 < e_2$ *is equivalent to* $q'_D(e_1) > q'_D(e_2)$.

Proof. We show that $e_1 < e_2$ implies $q'_D(e_1) - q'_D(e_2) > 0$. In fact, $q'_D(e_1) - q'_D(e_2) = \dfrac{e_1 + d/e_1}{m} - \dfrac{e_2 + d/e_2}{m} = \dfrac{(e_2 - e_1)(d - e_1e_2)}{e_1e_2m}$, where $m = 1,\ 2,\ 4$ as $d \equiv 2,\ 1,\ 3 \pmod 4$ respectively. Since $e_1 < e_2 < \sqrt{d}$, we get $q'_D(e_1) - q'_D(e_2) > 0$. The inverse is proved similarly. □

Lemma 4.8. *The number* q'_D *is the minimum of* $q'_D(e)$ *for all divisors* $e < \sqrt{d}$ *of* d.

Proof. Since $q'_D = q'_D(e)$ as e is the largest divisor of d less than $\sqrt{d}$, by Lemma 4.7, q'_D is the minimum of $q'_D(e)$. □

Proof of Theorem 4.5. Since q_D is a split prime, by Theorem 4.4, the condition $q_D = q'_D(e)$ for a divisor $e < \sqrt{d}$ of d is equivalent to the condition $f_D(x) = q_D^2$ for an integer x. Furthermore since q_D is the least split prime, using Lemmas 4.6 and 4.8, we get $q_D = q'_D(e) = q'_D$. □

By Theorems 2.5 and 4.5, we immediately show that (i) implies (vi) in Conjecture 1.1 as follows.

Corollary 4.9. *If $d \neq 1,\ 3$ and $d \equiv 1,\ 3 \pmod 4$, then $e_D \leqq 2$ implies $f_D(x) = q_D^2$ for an integer x.*

Further by Theorems 2.6 and 4.5, we have following corollary, which means that (vi) implies (v) in Conjecture 1.1.

Corollary 4.10. *If $d \neq 1,\ 3$ and $d \equiv 1,\ 3 \pmod 4$, then $f_D(x) = q_D^2$ implies $q_D > R_D$.*

Furthermore we can strengthen Corollary 4.10 as follows:

Proposition 4.11. (1) *If $d \equiv 1 \pmod 4$ and $f_D(x) = q_D^2$ for an integer x, then $q_D \geqq \sqrt{4+d}$.*

(2) *If $d \equiv 3 \pmod 4$ and $f_D(x) = q_D^2$ for an integer x, then $q_D \geqq \sqrt{\dfrac{1+d}{4}}$.*

Proof. (1) Suppose $d \equiv 1 \pmod 4$. By Lemma 4.3, if $f_D(x) = q_D^2$, then $x = \dfrac{d/e - e}{2}$ for a divisor $e < \sqrt{d}$ of d. Since $d \equiv 1 \pmod 4$, $d/e \equiv e \pmod 4$. Hence $d/e - e \geqq 4$, so $x = \dfrac{d/e - e}{2} \geqq 2$. Thus $f_D(x) \geqq f_D(2) = 4 + d$. Therefore $q_D \geqq \sqrt{4+d}$.
(2) Suppose $d \equiv 3 \pmod 4$. By Lemma 4.3, if $f_D(x) = q_D^2$, then $x = \dfrac{d/e - e - 2}{4}$ for a divisor $e < \sqrt{d}$ of d. Since $d/e - e \geqq 2$, we have $x = \dfrac{d/e - e - 2}{4} \geqq 0$, hence $f_D(x) \geqq f_D(0) = \dfrac{1+d}{4}$. Therefore $q_D \geqq \sqrt{\dfrac{1+d}{4}}$. □

In 1944, P.Papkovi [12] mentioned that if $d \equiv 3 \pmod 4$, then $e_D \leqq 2$ is equivalent to $q_D \geqq \sqrt{\dfrac{1+d}{4}}$. However he did not give any proof in his paper.

In Section 6, we state that $q_D > R_D$ implies $e_D \leqq 2$ under certain conjecture.

5. Properties related to split primes $q < \sqrt{D/3}$

In this section we consider imaginary quadratic fields K_D which have a split prime q less than $\sqrt{D/3}$. We may discuss only when $e_D = 2$ by the following result.

Proposition 5.1. (Mollin [11], p.122) *If $h_D = 1$, then $q_D > \sqrt{D/3}$.*

In Conjecture 1.1, we can not prove now that each of the conditions (ii)-(vi) is a sufficient condition for $e_D \leqq 2$. However we get the following equivalent conditions for $e_D = 2$ in K_D which has a split prime $q < \sqrt{D/3}$.

Theorem 5.2. *If $d \equiv 1,\ 3 \pmod 4$ and K_D has a split prime $q < \sqrt{D/3}$, then the following conditions are equivalent.*
(1) $e_D = 2$.
(2) *For every split prime $q < \sqrt{D/3}$, there exists a divisor $e < \sqrt{d}$ of d such that $q = q'_D(e)$.*
(3) *For every split prime $q < \sqrt{D/3}$, there exists an integer x such that $f_D(x) = q^2$.*

We give three lemmas for the proof of Theorem 5.2.

Lemma 5.3. *Suppose $d \equiv 1,\ 3 \pmod 4$. Let q be a split prime and $q = \mathfrak{q}\mathfrak{q}'$ the factorization of q to prime ideals. If $f_D(x) = q^2$ for an integer x, then $\mathfrak{q}$ and $\mathfrak{q}'$ are ambiguous.*

Proof. We may assume that $\mathfrak{q} = [q,\ x + \omega_D]$, where ω_D is defined by $\omega_D := \sqrt{-d}, (1 + \sqrt{-d})/2$ if $D \equiv 0,\ 3 \pmod 4$ respectively. Then $\mathfrak{q}$ is an ambiguous prime ideal since $f_D(x) = q^2$. By $q = \mathfrak{q}\mathfrak{q}'$, we have $q^2 = \mathfrak{q}^2\mathfrak{q}'^2$. Thus we get $\mathfrak{q}'^2 \sim 1$, so $\mathfrak{q}'$ is ambiguous. □

We have the following lemma by R.Sasaki.

Lemma 5.4. (Sasaki [16]) *Let $f_D(x) = p_1 p_2 \cdots p_r$ $(0 \leqq x \leqq D/4 - 1)$ the factorization of $f_D(x)$ to prime numbers and $p_i = \mathfrak{p}_i\mathfrak{p}'_i$ the factorization of p_i to prime ideals. Then ideal classes $[\mathfrak{p}_1]$, $[\mathfrak{p}_1\mathfrak{p}_2]$, $[\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3]$, $\cdots$, $[\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_r] = 1$ are mutually distinct.*

Further we have the following lemma.

Lemma 5.5. (cf. e.g. Shimizu and Goto [17]) *If q is any split prime less than $\sqrt{D/3}$, then there exist at least one integers x with $0 \leqq x \leqq D/4 - 1$ such that $f_D(x) \equiv 0 \pmod{q^2}$.*

Proof of Theorem 5.2. Möller [5] proved that (1) implies (2) at first, and Mollin [11] proved that (1) is equivalent to (2). In this paper we give another proof.

The equivalence of (2) and (3) is already stated as Theorem 4.4 without the condition $q < \sqrt{D/3}$.

First we show that (1) implies (3). Since q is a split prime less than $\sqrt{D/3}$, by Lemma 5.5, we may put $f_D(x) = q^2 c$ for an integer x with $0 \leqq x \leqq D/4 - 1$ and an integer $c \geqq 1$. If $c > 1$, then $\mathfrak{q}^2 \nsim 1$ or $\mathfrak{q}'^2 \nsim 1$ by Lemma 5.4, which is contradict to $e_D = 2$. Therefore $e_D = 2$ implies $f_D(x) = q^2$ for an integer x.

Secondly we show that (3) implies (1). If there exists an integer x such that $f_D(x) = q^2$, then by Lemma 5.3, $\mathfrak{q}$ and $\mathfrak{q}'$ are ambiguous for any split

prime $q < \sqrt{D/3}$, hence we get $e_D \leqq 2$. Furthermore by Proposition 5.1, we have $e_D \neq 1$ since $q < \sqrt{D/3}$. Hence we get $e_D = 2$. □

6. Properties related to the condition $q_D > R_D$

In Section 1, we mentioned the following relations between conditions of Conjecture 1.1.

$$\text{(i)} \Longrightarrow \text{(ii)} \Longrightarrow \text{(iii)}$$
$$\text{(i)} \Longrightarrow \text{(iv)} \iff \text{(vi)} \Longrightarrow \text{(v)}$$

In this section we consider the condition about $q_D > R_D$, namely (v) of Conjecture 1.1.

By the definition of p_D, we have $t_D \leqq p_D$. We want to prove that $q_D > R_D$ implies $p_D = t_D$, that is, (v) implies (ii) in Conjecture 1.1.

If $d \equiv 2 \pmod 4$, then as we stated in Theorem 3.4, $q_D > R_D$ is equivalent to $e_D \leqq 2$. Hence in this case we have that $q_D > R_D$ implies $p_D = t_D$.

If $d \equiv 1,\ 3 \pmod 4$, then we can not prove it now, but we have a weaker result.

Theorem 6.1. *If $d \neq 1,\ 3$ and $d \equiv 1,\ 3 \pmod 4$ and $q_D > R_D$, then $p_D \leqq t_D + 2$.*

For the proof of Theorem 6.1 we show the following lemmas.

Lemma 6.2. *If $d \neq 1,\ 3$ and $q_D > R_D$, then the number of split primes which divide $f_D(x)$ with $0 \leqq x \leqq D/4 - 1$ is at most three.*

Proof. First, we show $f_D(x) < (D/4)^2$ for any integer x with $0 \leqq x \leqq D/4 - 1$. If $d \neq 1$ and $d \equiv 1,\ 2 \pmod 4$, then $f_D(D/4-1) = (d-1)^2 + d = d^2 - (d-1) < d^2 = (D/4)^2$. If $d \neq 3$ and $d \equiv 3 \pmod 4$, then the interval $0 \leqq x \leqq D/4 - 1$ corresponds to $0 \leqq x \leqq (d-7)/4$ since x is an integer. Thus $f_D(\dfrac{d-7}{4}) = \left(\dfrac{d-7}{4}\right)^2 + \dfrac{d-7}{4} + \dfrac{1+d}{4} = \left(\dfrac{d}{4}\right)^2 - \left(\dfrac{3}{8}d - \dfrac{25}{16}\right)$. Since $d \geqq 7$, we have $\dfrac{3}{8}d - \dfrac{25}{16} > 0$. Hence $f_D(\dfrac{d-7}{4}) < \left(\dfrac{d}{4}\right)^2 = \left(\dfrac{D}{4}\right)^2$.

Assume the number of split prime factors of $f_D(x)$ is more than three for $0 \leqq x \leqq D/4 - 1$. Then $f_D(x) \geqq q_D^4$. If $d \equiv 2 \pmod 4$, then $f_D(x) \geqq q_D^4 > R_D^4 = D^2$. This is contradict to $f_D(x) < (D/4)^2$. If $d \equiv 1,\ 3 \pmod 4$, then $f_D(x) \geqq q_D^4 > R_D^4 = (D/4)^2$. This is contradict to $f_D(x) < (D/4)^2$. Hence the proof completes. □

Lemma 6.3. *If p is any prime divisor of D, then p^2 does not divide $f_D(x)$ for any integer x.*

Proof. Assume that p^2 divides $f_D(x)$ for an integer x. If $d \equiv 1,\ 2 \pmod 4$, then p divides both d and $f_D(x) = x^2 + d$. Therefore we get that p divides x^2, and so x. Thus p^2 divides x^2. Hence p^2 divides d, which is a contradiction. If $d \equiv 3 \pmod 4$, then $f_D(x) = \dfrac{(2x+1)^2 + d}{4}$. Similarly we get that p^2 divides $(2x+1)^2$. Hence p^2 divides d, which is a contradiction. Therefore p^2 does not divide $f_D(x)$ for any integer x. □

Proof of Theorem 6.1. Suppose $d \neq 1$ and $d \equiv 1 \pmod 4$. Then $f_D(x) = x^2 + d$, so $\nu(f_D(0)) = \nu(d) = t_D - 1$. Since $f_D(0) = d$, $f_D(x)$ is not divided by d for $0 < x \leqq D/4 - 1 = d - 1$. Let $f_D(x) = ap_1 \cdots p_r$ for $0 < x \leqq D/4 - 1$, where a is a product of prime factors of $D = 4d$ and p_i $(1 \leqq i \leqq r)$ is a split prime. By Lemma 6.3, a is square-free. Hence we get $\nu(a) \leqq t_D - 1$. Since $r \leqq 3$ by Lemma 6.2, we get $\nu(f_D(x)) \leqq t_D - 1 + 3 = t_D + 2$ for $0 < x \leqq D/4 - 1$. Therefore we get $p_D \leqq t_D + 2$.

Suppose $d \neq 3$ and $d \equiv 3 \pmod 4$. Since $f_D(x) = x^2 + x + \dfrac{1+d}{4}$ and $f_D(\dfrac{d-1}{2}) = d \cdot \dfrac{1+d}{4}$, $f_D(x)$ is not divided by d for $0 \leqq x \leqq D/4 - 1$. Let $f_D(x) = ap_1 \cdots p_r$ as above. By Lemma 6.3, we get $\nu(a) \leqq t_D - 1$. Since $r \leqq 3$, we get $\nu(f_D(x)) \leqq t_D - 1 + 3 = t_D + 2$. Therefore $p_D \leqq t_D + 2$. □

Under the condition $q_D > R_D$, we have the following results about $q'_D(e)$.

Proposition 6.4. (1) *If $d \neq 1$, $d \equiv 1,\ 2 \pmod 4$ and $q_D > R_D$, then $q'_D(e)$ is a prime for any divisor $e < \sqrt{d}$ of d.*
(2) *If $d \neq 3$, $d \equiv 3 \pmod 4$ and $q_D > R_D$, then $q'_D(e)$ is a prime or $q'_D(e) = q_D^2 = (1+d)/4$ for any divisor $e < \sqrt{d}$ of d.*

Proof. Assume $d \neq 1,\ 3$ and $q'_D(e)$ is not a prime. Then by Lemma 4.6, $q'_D(e)$ has at least two split prime factors. Hence we get $q'_D(e) \geqq q_D^2$.

(1) If $d \equiv 2 \pmod 4$, then by Lemma 4.7, we have $q'_D(e) \leqq 1 + d$ and $q'_D(e) \geqq q_D^2 > R_D^2 = 4d$. Hence $4d < q'_D(e) \leqq 1 + d$, so $4d < 1 + d$, which is a contradiction. Therefore $q'_D(e)$ is a prime.

If $d \equiv 1 \pmod 4$, then by Lemma 4.7, we have $q'_D(e) \leqq (1+d)/2$ and $q'_D(e) \geqq q_D^2 > R_D^2 = d$. Hence $d < q'_D(e) \leqq (1+d)/2$, which is a contradiction. Therefore $q'_D(e)$ is a prime.

(2) If $d \equiv 3 \pmod 4$, then by Lemma 4.7, we have $q'_D(e) \leqq (1+d)/4$ and $q'_D(e) \geqq q_D^2 > R_D^2 = d/4$. Hence $d/4 < q'_D(e) \leqq (1+d)/4$, which is possible only when $q'_D(e) = (1+d)/4$. Then since $d/4 < q_D^2 \leqq q'_D(e) = (1+d)/4$, we obtain $q'_D(e) = q_D^2 = (1+d)/4$, and otherwise $q'_D(e)$ is a prime. □

As we stated in Lemma 5.5, there is an integer x in the interval $0 \leqq x \leqq D/4 - 1$ such that $f_D(x) \equiv 0 \pmod{q^2}$ for any split prime $q < \sqrt{D/3}$.

Replacing the interval $0 \leqq x \leqq D/4 - 1$ with $0 \leqq x < q$, we have the following conjecture:

Conjecture 6.5. *Suppose that* $d \equiv 1,\ 3 \pmod 4$ *and* K_D *has a split prime* $q < \sqrt{D/3}$. *If* $q_D > R_D$ *and* $q < \sqrt{D/3}$ *is any split prime, then* $f_D(x) \equiv 0 \pmod{q^2}$ *for an integer* x *with* $0 \leqq x < q$.

Assuming Conjecture 6.5, we show the following theorem.

Theorem 6.6. *Suppose that* $d \equiv 1,\ 3 \pmod 4$ *and* K_D *has a split prime* $q < \sqrt{D/3}$. *If Conjecture* 6.5 *is true, then the following conditions are equivalent.*
(1) $q_D > R_D$.
(2) *For every split prime* $q < \sqrt{D/3}$, *there is an integer* x *such that* $f_D(x) = q^2$.

Proof. First we prove that (2) implies (1), without Conjecture 6.5. Since we assume $f_D(x) = q^2$ for every split prime $q < \sqrt{D/3}$, we have $f_D(x) = q_D^2$ for an integer x. Hence by Corollary 4.10, we get $q_D > R_D$.

Conversely we assume $q_D > R_D$.

(i) Suppose $d \equiv 1 \pmod 4$. Since $q_D > R_D$, we get $q \geqq q_D > \sqrt{D/4} = \sqrt{d}$. By Conjecture 6.5, set $f_D(x) = q^2c$ for an integer x with $0 \leqq x < q$ and an integer c. If $c > 1$, then $f_D(x) = q^2c \geqq 2q^2$. Furthermore since $0 \leqq x < q$, $f_D(x) = x^2 + d < q^2 + d$. Hence $2q^2 < q^2 + d$, so $q < \sqrt{d}$, which is a contradiction. Therefore we have $c = 1$, hence $f_D(x) = q^2$ for an integer x.

(ii) Suppose $d \equiv 3 \pmod 8$. Since $q_D > R_D$, then $q_D > \sqrt{D/4} = \sqrt{d/4}$. By Conjecture 6.5, set $f_D(x) = q^2c$ for an integer x with $0 \leqq x < q$ and an integer c. In this case $f_D(x)$ is odd, so if $c > 1$, then $c \geqq 3$ and $f_D(x) = q^2c \geqq 3q^2$. Since $0 \leqq x < q$, $f_D(x) = x^2+x+\dfrac{1+d}{4} < q^2+q+\dfrac{1+d}{4} = q^2+q+\dfrac{1}{4}+\dfrac{d}{4}$. Since $q \geqq q_D > \sqrt{d/4}$, $q^2 + q + \dfrac{1}{4} + \dfrac{d}{4} < q^2 + q + \dfrac{1}{4} + q^2 = 2q^2 + q + \dfrac{1}{4}$. Hence $3q^2 < 2q^2 + q + \dfrac{1}{4}$, so $q^2 < q + \dfrac{1}{4}$, which is impossible.

(iii) Suppose $d \equiv 7 \pmod 8$. We can prove without Conjecture 6.5. In this case we have $q_D = 2$ and $R_D = \sqrt{d/4}$. Thus $q_D > R_D$ implies $d = 7$ or $d = 15$. If $d = 7$, then there are no split primes less than $\sqrt{D/3}$. If $d = 15$, then there is only one split prime $q < \sqrt{D/3}$, namely $q = q_D = 2$. Thus $f_D(0) = 2^2 = q^2$.

Therefore we prove that (1) implies (2). □

Corollary 6.7. *Under Conjecture* 6.5, *if* $d \equiv 1,\ 3 \pmod 4$, *then* $q_D > R_D$ *is equivalent to* $e_D \leqq 2$.

Proof. It is sufficient that we prove that $q_D > R_D$ implies $e_D \leqq 2$. If K_D has a split prime $q < \sqrt{D/3}$, then by Theorems 6.6 and 5.2 we get $e_D = 2$. If K_D has no split primes less than $\sqrt{D/3}$, then $e_D \leqq 2$. □

If Conjecture 6.5 is true, then by Theorem 2.5, 2.6, 4.5 and Corollary 6.7, we get the equivalence of some conditions in Conjecture 1.1.

Corollary 6.8. *Under Conjecture* 6.5*, if* $d \neq 1,\ 3$ *and* $d \equiv 1,\ 3 \pmod 4$*, then the following conditions are equivalent.*
(1) $e_D \leqq 2$.
(2) $q_D = q'_D$.
(3) $q_D > R_D$.
(4) $f_D(x) = q_D^2$ *for an integer* x.

References

[1] S. Chowla, J. Cowles and M. Cowles : The Least Prime Quadratic Residue and the Class Number, J. Number Theory **22**, 1-3 (1986)
[2] J. Cohen and J. Sonn : On the Ono invariants of imaginary quadratic fields, J. Number Theory **95**, 259-267 (2002)
[3] F. G. Frobenius : Über quadratische Formen, die viele Primzahlen darstellen, Sitzungsber. d. Königl. Akad. d. Wiss. zu Berlin, 966-980 (1912)
[4] M. D. Hendy : Prime quadratics associated with complex quadratic fields of class number two. Proc. Amer. Math. Soc.**43**, 253-260 (1974)
[5] H. Möller : Verallgemeinerung eines Satzes Rabinowitsch über imaginär-quadratische Zahlkörper, J. Reine Angew. Math. **285** (1976), 100-113.
[6] R. A. Mollin : Orders in quadratic fields I, Proc. Japan Acad. **69A**, 45-48 (1993).
[7] R. A. Mollin and L.-C. Zhang : Orders in quadratic fields II, Proc. Japan Acad. **69A**, 368-371 (1993).
[8] R. A. Mollin : Orders in quadratic fields III, Proc. Japan Acad. **70A**, 176-181 (1994).
[9] R. A. Mollin : Orders in quadratic fields IV, Proc. Japan Acad. **71A**, 131-133 (1995).
[10] R. A. Mollin : Orders in quadratic fields V, Proc. Japan Acad. **71A**, 182-183 (1995).
[11] R. A. Mollin : Quadratics, CRC Press, (1995).
[12] P. Papkovi : On imaginary quadratic fields admitting only ambiguous classes, Bull. Acad. Sci. Georgian SSR. **5**, (1944), 585-592. (Russian)
[13] G. Rabinowitsch : Eindeutigkeit der Zerlegung in Primzahlfaktoren in quadratischen Zahlkörpern, J. Reine Angew. Math. **142** (1913), 153-164.
[14] F. Sairaiji and K. Shimizu : A note on Ono's numbers associated to imaginary quadratic fields, Proc. Japan Acad. **77A**, 29-31 (2001).
[15] F. Sairaiji and K. Shimizu : An inequality between class numbers and Ono's numbers associated to imaginary quadratic fields, Proc. Japan Acad. **78A**, 105-108 (2002).
[16] R. Sasaki : On a lower bound for the class number of an imaginary quadratic field, Proc. Japan Acad. Ser. A **62** (1986), 37-39.
[17] K. Shimizu and K. Goto : A Property of Integers Related to Quadratic Fields, J. Fac. Educ. Tottori Univ, **47**, 5-12 (1998)

Kenichi Shimizu
Kenmei Girls' Junior and Senior High School
Himeji, 670-0012 Japan
e-mail address: s-2357@mh1.117.ne.jp

(*Received October 1, 2006*)
(*Revised January 26, 2007*)