RIMS Kôkyûroku Bessatsu
B32 (2012), 255–269

Imaginary quadratic fields whose exponents are less than or equal to two, II

By

Kenichi SHIMIZU *

Abstract

Shimizu [14] gave some necessary conditions for $e_D \leqq 2$, where e_D is the exponent of the ideal class group of an imaginary quadratic field $\mathbf{Q}(\sqrt{-D})$. In this paper we mainly consider some relations between prime-producing polynomials and the condition $e_D \leqq 2$. First we give a generalization of Mollin's result. Next we consider the inverse of Mollin's result when $d \equiv 2 \pmod 4$ and $t_D = 3$, and give some relations between invariants of $\mathbf{Q}(\sqrt{-D})$.

§ 1. Introduction

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 e_D the exponent of the ideal class group of K_D that is the least positive integer n such that $\mathfrak{a}^n$ are principal for all ideals $\mathfrak{a}$. We denote by t_D the number of different prime factors of D.

We call a rational prime q a split prime if $(q) = \mathfrak{q}\mathfrak{q}'$ ($\mathfrak{q} \neq \mathfrak{q}'$) and a ramified prime if $(q) = \mathfrak{q}^2$ for prime ideals $\mathfrak{q}$ and $\mathfrak{q}'$ in K_D. Let q_D denote the least split prime.

We define $f_D(x)$ by

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

Received April 1, 2011. Revised November 19, 2011.
2000 Mathematics Subject Classification(s): Primary 11R11, Secondary 11R29
Key Words: *imaginary quadratic field, exponent, prime-producing polynomial*
Supported by JAPAN SUPPORT
*e-mail: s-2357@gaia.eonet.ne.jp

then we have that prime divisors of $f_D(x)$ are split primes or ramified primes (Lemma 3.2).

Further for every divisor e 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 by q'_D the minimum of $q'_D(e)$ for all divisors e of d. We have that $q'_D(e)$ and q'_D are split primes (see Shimizu [14]).

Let b be any divisor of d and $a = d/b$. We assume $b > 1$. Let p be the least prime divisor of b, then we define I_b by

$$I_b := \begin{cases} \{x \mid 0 \leqq x \leqq p-1\} & \text{if } d \equiv 2 \pmod 4 \text{ and } b \text{ is a prime} \\ \{x \mid 0 < x \leqq p-1\} & \text{if } d \equiv 2 \pmod 4 \text{ and } b \text{ is not a prime} \\ \{x \mid 0 \leqq x \leqq \dfrac{p}{2} - 1\} & \text{if } d \equiv 1 \pmod 4 \\ \{x \mid 0 \leqq x \leqq \dfrac{p}{4} - \dfrac{1}{2} - \dfrac{p}{2d}\} & \text{if } d \equiv 3 \pmod 4, \end{cases}$$

where x are integers.

We define quadratic polynomials $f_{D,b}(x)$ by

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

In Lemma 3.3, we show that the value of $f_{D,b}(x)$ in I_b is a split prime or a product of split primes.

We denote by $\nu(n)$ the number of (not necessarily different) prime factors of an integer n, and define the Ono number p_D as follows,

$$p_D := \begin{cases} \max\{\nu(f_D(x)) \mid x \text{ are integers in } 0 \leqq x \leqq D/4 - 1 & \text{if } d \neq 1, 3 \\ 1 & \text{if } d = 1, 3. \end{cases}$$

In this paper we assume $d \neq 1,\ 3$ through all sections.

For these invariants, we pose the following conjecture:

Conjecture 1.1. *The following conditions* (i) $\sim$ (vi) *are equivalent.*

(i) $e_D \leqq 2$.

(ii) $p_D = t_D$.

(iii) *For every divisor b of d, $f_{D,b}(x)$ takes only prime values for all integers x with I_b.* (We call this condition GEP-property in this paper.)

(iii)$'$ *For the largest prime divisor b of d, $f_{D,b}(x)$ takes only prime values for all integers x with I_b.* (We call this condition EP-property in this paper.)

(iv) $q_D = q'_D$.

(v) $q_D > \sqrt{D/4}$.

(vi) $f_D(x) = q_D^2$ *for an integer x.* (*Only when* $d \equiv 1,\ 3 \pmod 4$)

Similar conjecture was given by Shimizu [14], two conditions are improved in this paper as follows.

In [14], we did not have the condition (iii), and we wrote the condition $q_D > R_D$ instead of (v), where R_D is $\sqrt{D}$ or $\sqrt{D/4}$ when $d \equiv 2 \pmod 4$ or $d \equiv 1,\ 3 \pmod 4$, respectively.

We here note that some relations have been known between those conditions of Conjecture 1.1. G.Rabinowitsch [10] and F.G.Frobenius [1] showed independently that (i) $\Leftrightarrow$ (iii)$'$ when $t_D = 1$. M.D.Hendy [4] essentially showed that (i) $\Leftrightarrow$ (iii)$'$ when $t_D = 2$. H.Möller [5] proved that (i) $\Rightarrow$ (iv) and (iv) $\Rightarrow$ (v). R.A.Mollin [6][7][8] showed that (i) $\Rightarrow$ (ii) and (ii) $\Rightarrow$ (iii)$'$. Shimizu [14] showed that (i) $\Rightarrow$ (vi) and (iv) $\Leftrightarrow$ (vi) when $d \equiv 1, 3 \pmod 4$, and showed that (i) and (iv) are equivalent when $d \equiv 2 \pmod 4$. X.Guo and H.Qin [3] showed that (i) $\Leftrightarrow$ (ii) when $t_D = 3$ under the Extended Riemann Hypothesis.

In Section 3 we show that (i) $\Rightarrow$ (iii) (Theorem 3.1), which is a generalization of Mollin's result. In Section 4, we show that (v) $\Rightarrow$ (iv) when $d \equiv 1,\ 2 \pmod 4$ (Theorem 4.2). In Section 5, only when $t_D = 3$ and $d \equiv 2 \pmod 4$, we show that (iii)$'$ $\Rightarrow$ (i) (Theorem 5.1) and that conditions in Conjecture 1.1 are equivalent except (vi) (Theorem 5.4). Consequently by Theorem 5.4 we obtain the same result as X.Guo and H.Qin [3] without the Extended Riemann Hypothesis in the case of $d \equiv 2 \pmod 4$. In Section 6, we show that (iii)$'$ $\Rightarrow$ (v) when $t_D = 3$ and $d \equiv 1 \pmod 4$ (Theorem 6.1).

§ 2. Prime-producing polynomials

In this section we sketch the history of prime-producing polynomials.

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

In 1912, F.G.Frobenius [1] and G.Rabinowitsch [10] independently showed that the above fact is related to the class number of imaginary quadratic field $\mathbf{Q}(\sqrt{1 - 4A})$. They proved:

Theorem 2.1. *The following* (1) *and* (2) *are equivalent.*
(1) *The quadratic polynomial* x^2+x+A $(A \geqq 2)$ *takes only prime values for all integers with* $0 \leqq x \leqq A-2$.
(2) $\mathbf{Q}(\sqrt{1-4A})$ *has class number one.*

In the same paper, Frobenius referred to prime-producing polynomials related to imaginary quadratic fields with $h_D = 2$ as follows.

Theorem 2.2. *Let* p *be an odd prime number.*
(i) *If* $\mathbf{Q}(\sqrt{-2p})$ *has class number two, then* $2x^2+p$ *takes only prime values for all integers with* $0 \leqq x < p$.
(ii) *If* $p \equiv 1 \pmod 4$ *and* $\mathbf{Q}(\sqrt{-p})$ *has class number two, then* $2x^2-2x+(p+1)/2$ *takes only prime values for all integers with* $0 \leqq x < (p+1)/2$.

In 1974, M.D.Hendy [4] gave a necessary and sufficient condition for prime-producing polynomials related to imaginary quadratic fields with $h_D = 2$ as follows.

Theorem 2.3. *Let* p *and* q *be odd prime numbers.*
(i) *If* $\mathbf{Q}(\sqrt{-2p})$ *has class number two if and only if* $2x^2+p$ *is prime for all integers with* $0 \leqq x \leqq \sqrt{p/2}$.
(ii) *If* $p \equiv 1 \pmod 4$ *and* $\mathbf{Q}(\sqrt{-p})$ *has class number two if and only if* $2x^2+2x+(p+1)/2$ *is prime for all integers with* $0 \leqq x \leqq (\sqrt{p}-1)/2$.
(iii) *If* $pq \equiv 3 \pmod 4$, $p < q$ *and* $\mathbf{Q}(\sqrt{-pq})$ *has class number two if and only if* $px^2+px+(p+q)/4$ *is prime for all integers with* $0 \leqq x \leqq \sqrt{pq/12}-1/2$.

In 1995, R.A.Mollin [7][8] generalized these results to imaginary quadratic fields whose class numbers are more than two. He considered imaginary quadratic fields with $h_D = 2^{t_D-1}$. It is known that $h_D = 2^{t_D}$ is equivalent to $e_D \leqq 2$. From now on we use $e_D \leqq 2$ instead of $h_D = 2^{t_D-1}$.

Mollin proved the following.

Theorem 2.4. (Mollin [6], [7] p.110)
If $e_D \leqq 2$, *then the equality* $p_D = t_D$ *holds.*

Using $f_{D,b}(x)$, we state Mollin's result.

Theorem 2.5. (Mollin [7] p.115-116, [8]) *Let* b *be the largest prime divisor of* d *and* $a=d/b$. *If* $e_D \leqq 2$, *then* $f_{D,b}(x)$ *takes only prime values for all integers* x *with* I_b.

Theorem 2.5 is proved by using Theorem 2.4.

§ 3. A generalization of Mollin's result

In this section we give a generalization of Theorem 2.5. Though we have taken b the largest prime divisor of d in Theorem 2.5, we can take b any divisor of d as follows.

Theorem 3.1. *Let $b > 1$ be any divisor of d, $a = d/b$ and p the least prime divisor of b. We assume $a > 1$ when $d \equiv 3 \pmod 4$ and d is not a prime. If $e_D \leqq 2$, then the quadratic polynomial $f_{D,b}(x)$ takes only prime values for all integers x with I_b.*

When $d \equiv 3 \pmod 4$ and d is not a prime, if $a = 1$, then there are counter examples. For example, if $d = 15$, then $f_{D,b}(x) = x^2 + x + 4$ does not take prime values x in I_b.

If b is the largest prime divisor of d, then Theorem 3.1 gives Theorem 2.5.

For the proof of Theorem 3.1, we give the following lemmas.

Lemma 3.2. *Prime divisors of $f_D(x)$ are split primes or ramified primes. Conversely all split primes and all ramified primes divide $f_D(x)$ for some integers x.*

Proof. At first, we consider in the case of $d \equiv 1,\ 2 \pmod 4$. Let p be a prime which does not divide D, then we have that p is odd and that

$$\begin{aligned} p \mid f_D(x) &\Longleftrightarrow x^2 + d \equiv 0 \pmod p, \\ &\Longleftrightarrow X^2 \equiv -D \,(\mathrm{mod}\ p) \text{ is solvable}, \\ &\Longleftrightarrow p \text{ is a split prime.} \end{aligned}$$

If $p \mid D$, then p is a ramified prime. When $d \equiv 2 \pmod 4$ we have

$$p \mid D \Longleftrightarrow p \mid f_D(0)$$

. When $d \equiv 1 \pmod 4$ we have

$$p \mid D \Longleftrightarrow \begin{cases} p \mid f_D(0) \text{ for an odd prime } p, \\ p \mid f_D(1) \text{ for } p = 2. \end{cases}$$

Second, we consider in the case of $d \equiv 3 \pmod 4$. For an odd prime p we have

$$\begin{aligned} p \mid f_D(x) &\Longleftrightarrow x^2 + x + \frac{1+d}{4} = \frac{(2x+1)^2 + d}{4} \equiv 0 \pmod p, \\ &\Longleftrightarrow (2x+1)^2 \equiv -d \pmod p, \\ &\Longleftrightarrow X^2 \equiv -D \,(\mathrm{mod}\ p) \text{ is solvable}, \\ &\Longleftrightarrow p \text{ is a split prime.} \end{aligned}$$

For $p = 2$, when $d \equiv 7 \pmod 8$ we have that 2 is a split prime and $2 \mid f_D(x)$ for all x. When $d \equiv 3 \pmod 8$ we have that 2 is neither a split prime nor a ramified prime, and $2 \nmid f_D(x)$ for all x. Thus we complete the proof. $\square$

Lemma 3.3. *In I_b, the value of the quadratic polynomial $f_{D,b}(x)$ is a split prime or a product of split primes.*

Proof. At first, we state a relation of $f_D(x)$ and $f_{D,b}(x)$. When $d \equiv 2 \pmod 4$ we have $f_D(ax) = a^2x^2 + d = a(ax^2 + b) = af_{D,b}(x)$.

When $d \equiv 1 \pmod 4$ we have $f_D(2ax + a) = 4a^2x^2 + 4a^2x + a^2 + d = 2a\Big(2ax^2 + 2ax + \frac{a+b}{2}\Big) = 2af_{D,b}(x)$.

When $d \equiv 3 \pmod 4$, since $f_D(x) = x^2 + x + \frac{1+d}{4} = \frac{(2x+1)^2 + d}{4}$, we have

$$\begin{aligned} f_D(ax + \frac{a-1}{2}) &= \frac{(2ax+a)^2 + d}{4} \\ &= a\Big(ax^2 + ax + \frac{a+b}{4}\Big) = af_{D,b}(x). \end{aligned}$$

Therefore by Lemma 3.2, we get that prime divisors of $f_{D,b}(x)$ are split primes or ramified primes.

Next we show that no ramified primes divide $f_{D,b}(x)$.

Assuming that $f_{D,b}(x)$ is divided by a prime divisor p' of d, we derive a contradiction.

It holds that a and b have no common prime divisors since d is square-free. Let p be the least prime factor of b.

When $d \equiv 2 \pmod 4$ we have $f_{D,b}(x) = ax^2 + b$. By $p' \mid (ax^2+b)$, $p' \mid a$ immediately implies $p' \mid b$, which is a contradiction. If $p' \mid b$, then $p' \mid ax^2$. Since $x \in I_b$, namely, $0 < x < p \leqq p'$, we get $p' \mid a$, which is a contradiction.

When $d \equiv 1 \pmod 4$ we have

$$f_{D,b}(x) = 2ax^2 + 2ax + \frac{a+b}{2}.$$

We show that the values of $f_{D,b}(x)$ are odd. By $d = ab \equiv 1 \pmod 4$, it holds that $a \equiv b \equiv 1 \pmod 4$ or $a \equiv b \equiv 3 \pmod 4$. Hence we get $a + b \equiv 2 \pmod 4$, and so the values of $f_{D,b}(x)$ are odd.

As we assume $p' \mid f_{D,b}(x)$, $p' \mid a$ implies $p' \mid (a + b)$. Hence we have $p' \mid b$, which is a contradiction.

On the other hand, from $p' \mid f_{D,b}(x)$ we have $p' \mid (4ax^2 + 4ax + a + b)$. If $p' \mid b$, then we have

$$\begin{aligned} 4ax^2 + 4ax + a + b &\equiv 4ax^2 + 4ax + a \\ &\equiv a(2x+1)^2 \equiv 0 \pmod{p'}. \end{aligned}$$

Hence we have $p' \mid (2x + 1)$ since $p' \nmid a$. By $x \in I_b$, namely, $0 \leqq x \leqq p/2 - 1$, we have $0 < 2x + 1 \leqq p - 1 \leqq p' - 1$, which is contradict to $p' \mid (2x + 1)$.

Finally, when $d \equiv 3 \pmod 4$ we have

$$f_{D,b}(x) = ax^2 + ax + \frac{a+b}{4}.$$

As we assume $p' \mid f_{D,b}(x)$, $p' \mid a$ implies $p' \mid b$, which is a contradiction. If $p' \mid b$, then

$$\begin{aligned} ax^2 + ax + \frac{a+b}{4} &= \frac{a(2x+1)^2 + b}{4} \\ &\equiv \frac{a(2x+1)^2}{4} \equiv 0 \pmod{p'}. \end{aligned}$$

Hence we get $p' \mid a(2x+1)^2$. Thus we have $p' \mid (2x+1)$ since $p' \nmid a$. From $x \in I_b$, namely, $0 \leqq x \leqq p/4 - 1/2 - p/(2d)$, we have

$$0 < 2x + 1 \leqq \frac{p}{2} - \frac{p}{d} < p \leqq p',$$

which is contradict to $p' \mid (2x+1)$. Thus we complete the proof. $\square$

Möller gave an lower bound for q_D.

Theorem 3.4. (Möller [5]) *If $e_D \leqq 2$, then $q_D > \sqrt{D}$ or $q_D > \sqrt{D/4}$ when $d \equiv 2$ or $d \equiv 1,\ 3 \pmod 4$, respectively.*

Using Lemma 3.3 and Theorem 3.4, we prove Theorem 3.1.

Proof. (Theorem 3.1) We prove this theorem by two steps. First, assume that b is a prime divisor of d, second, assume that b is not a prime.

Step I: Let b be a prime divisor of d. When $d \equiv 2 \pmod 4$ we have $f_D(ax) = af_{D,b}(x)$. By Theorem 2.4 we have $p_D = t_D$, and $\nu(a) = t_D - 1$ since b is a prime divisor of d. Hence we get that $f_{D,b}(x)$ takes only prime values for all integers x with $0 \leqq ax \leqq D/4 - 1 = d - 1$, which corresponds to $0 \leqq x \leqq d/a - 1/a = b - 1/a$, that is, $0 \leqq x \leqq b - 1$. Therefore $f_{D,b}(x)$ takes only prime values for all integers x with I_b.

Next, when $d \equiv 1 \pmod 4$ we have $f_D(2ax + a) = 2af_{D,b}(x)$. Since $p_D = t_D$ and $\nu(2a) = t_D - 1$, we get that $f_{D,b}(x)$ takes only prime values for all integers x with $0 \leqq 2ax + a \leqq D/4 - 1 = d - 1$, which corresponds to $0 \leqq x \leqq d/2a - 1/2a - 1/2$, that is, $0 \leqq x \leqq b/2 - 1$. Therefore $f_{D,b}(x)$ takes only prime values for all integers x with I_b.

Last, when $d \equiv 3 \pmod 4$ we have $f_D(ax + \dfrac{a-1}{2}) = af_{D,b}(x)$. From $p_D = t_D$ and $\nu(a) = t_D - 1$, we get that $f_{D,b}(x)$ takes only prime values for all integers x with $0 \leqq ax + (a-1)/2 \leqq D/4 - 1 = d/4 - 1$, which corresponds to $0 \leqq x \leqq d/(4a) - 1/2 - 1/(2a)$, that is, $0 \leqq x \leqq b/4 - 1/2 - b/(2d)$. Therefore $f_{D,b}(x)$ takes only prime values for all integers x with I_b.

Step II: Let b be not a prime and p the least prime divisor of b, then it holds $ap^2 < ab = d$. We assume that there is an integer x such that $f_{D,b}(x)$ is not a prime in I_b, and let $f_{D,b}(x) = q_1 \cdots q_r$ (q_i is a split prime, $1 \leqq i \leqq r$ and $r \geqq 2$) by Lemma 3.3. Then we have $f_{D,b}(x) \geqq q_D^2$.

At first, when $d \equiv 2 \pmod 4$ we have $f_{D,b}(x) = ax^2 + b \geqq q_D^2$. Since $e_D \leqq 2$, we have $q_D^2 > D = 4d$ by Theorem 3.4. Hence we get $4d < q_D^2 \leqq ax^2 + b$. On the other hand, since $x < p$ and $ap^2 < d$, we get

$$ax^2 + b < ap^2 + b < d + b.$$

Therefore we have $4d < d + b$, which is a contradiction. Hence $f_{D,b}(x)$ takes only prime values for all integers x with I_b.

Second, when $d \equiv 1 \pmod 4$ we have $f_{D,b}(x) = 2ax^2 + 2ax + (a+b)/2 \geqq q_D^2$. Since $x \leqq p/2 - 1$, $ap^2 < d$ and $a + b \leqq 1 + d$, we have

$$\begin{aligned}
&2ax^2 + 2ax + \frac{a+b}{2} \\
&\leqq 2a\left(\frac{p}{2} - 1\right)^2 + 2a\left(\frac{p}{2} - 1\right) + \frac{1+d}{2} \\
&= 2a\left(\frac{p^2}{4} - p + 1\right) + ap - 2a + \frac{1+d}{2} \\
&= \frac{ap^2}{2} - ap + \frac{1+d}{2} \\
&< \frac{d}{2} + \frac{1+d}{2} = d + \frac{1}{2}.
\end{aligned}$$

Hence $2ax^2 + 2ax + (a+b)/2 \leqq d$. By Theorem 3.4 we have $q_D^2 > D/4 = d$, therefore we get

$$d < q_D^2 \leqq 2ax^2 + 2ax + \frac{a+b}{2} \leqq d,$$

which is a contradiction.

Finally, when $d \equiv 3 \pmod 4$ we have $f_{D,b}(x) = ax^2 + ax + (a+b)/4 \geqq q_D^2$. By Theorem 3.4, we have $q_D^2 > D/4 = d/4$. Since $x \leqq p/4 - 1/2 - p/(2d)$ and $ap^2 < d$, we get

$$\begin{aligned}
&ax^2 + ax + \frac{a+b}{4} = \frac{a(2x+1)^2 + b}{4} \\
&\leqq \frac{a}{4}\left(\frac{p}{2} - \frac{p}{d}\right)^2 + \frac{b}{4} \\
&= \frac{ap^2}{4}\left(\frac{1}{2} - \frac{1}{d}\right)^2 + \frac{b}{4} < \frac{d}{4}\left(\frac{1}{4} - \frac{1}{d} + \frac{1}{d^2}\right) + \frac{b}{4} \\
&= \frac{d}{16} - \frac{1}{4} + \frac{1}{4d} + \frac{b}{4} < \frac{d}{16} + \frac{b}{4}.
\end{aligned}$$

In this case, since we assume $a > 1$, we have $a \geqq 3$. Thus we have $b \leqq d/3$. Therefore

$$\frac{d}{16} + \frac{b}{4} \leqq \frac{d}{16} + \frac{d}{12} = \frac{7}{48}d < \frac{d}{4}.$$

Hence we get

$$\frac{d}{4} < q_D^2 \leqq ax^2 + ax + \frac{a+b}{4} < \frac{d}{4},$$

which is a contradiction. Thus we complete the proof of Theorem 3.1. $\square$

§ 4. On the condition $q_D > \sqrt{D/4}$

In this section we show Theorem 4.2 below. For the proof of Theorem 4.2 we give the following lemma.

Lemma 4.1. *For an odd split prime q there are two integers x in $0 \leqq x < q$ such that $q \mid f_D(x)$. If $d \equiv 1,\ 2 \pmod 4$, then they are positive, and one is even and the other is odd. If $d \equiv 3 \pmod 4$, then they are non-negative, and both even or both odd.*

Proof. By Lemma 3.2, there are integers x such that $q \mid f_D(x)$. When $d \equiv 1,\ 2 \pmod 4$, since $q \nmid f_D(0)$ we may put x_0 the least positive integers such that $q \mid f_D(x_0)$. Since $f_D(q - x_0) = (q - x_0)^2 + d = q(q - 2x_0) + f_D(x_0)$, we get that $q \mid f_D(x_0)$ implies $q \mid f_D(q - x_0)$. Then we have that two integers x_0 and $q - x_0$ are different, for $x_0 = q - x_0$ implies $2x_0 = q$, which is impossible since q is odd. Thus we get $0 < x_0 < q/2 < q - x_0 < q$. Therefore there are two integers x in $0 < x < q$ such that $q \mid f_D(x)$, and one of them is even and the other odd since q is odd.

When $d \equiv 3 \pmod 4$, let x_0 be the least non-negative integers such that $q \mid f_D(x_0)$. We have:

$$\begin{aligned} f_D(q-1-x_0) &= (q-1-x_0)^2 + (q-1-x_0) + (1+d)/4 \\ &= q\{q-1-2x_0\} + x_0^2 + x_0 + (1+d)/4 \\ &= q\{q-1-2x_0\} + f_D(x_0), \end{aligned}$$

hence we get that $q \mid f_D(x_0)$ implies $q \mid f_D(q-1-x_0)$. Assuming $x_0 = q-1-x_0$, we have $x_0 = (q-1)/2$ and $f_D(x_0) = (q^2+d)/4$. Thus by $q \mid f_D(x_0)$ we get $q \mid d$, which is a contradiction. Thus we obtain $x_0 < q-1-x_0$, that is, $0 \leqq x_0 < (q-1)/2 < q-1-x_0 < q$. Hence there are two integers x in $0 \leqq x < q$ such that $q \mid f_D(x)$. Further we obtain that both x_0 and $q-1-x_0$ are even or both odd since q is odd. $\square$

Theorem 4.2. *Suppose* $d \equiv 1,\ 2 \pmod 4$. *If* $q_D > \sqrt{D/4}$, *then* $q_D = q'_D$.

Proof. When $d \equiv 1,\ 2 \pmod 4$, we have that q_D is odd, and that there are two integers x in $0 < x < q_D$ such that $q_D \mid f_D(x)$ by Lemma 4.1.

First, we prove the theorem when $d \equiv 2 \pmod 4$. Assume that x is even, then we have that $x^2 + d$ is even, hence we put $x^2 + d = 2q_D c$ ($c \geqq 1$).

If c is divided by a split prime, then $x^2 + d \geqq 2q_D^2$. By $q_D > x$ we get $q_D^2 + d > x^2 + d \geqq 2q_D^2$, hence we obtain $q_D^2 + d > 2q_D^2$, and so $q_D < \sqrt{D/4}$. Therefore $q_D > \sqrt{D/4}$ implies that $c = 1$ or the divisors of c are only ramified primes. Since x is even, it holds $x^2 + d \equiv 2 \pmod 4$. Hence we have $4 \nmid (x^2 + d)$, and so c is odd. Then an odd ramified prime p divides c exactly, because $p^2 \mid c$ implies $p^2 \mid d$, which is impossible since d is square-free. Thus we get $2c \mid d$, and so $2c \mid x$. Putting $x = 2cx_1$, we have $4c^2x_1^2 + d = 2q_D c$, hence we get $2cx_1^2 + d/(2c) = q_D$. Since $x_1 \geqq 1$, we have $q_D \geqq 2c + d/(2c) = q'_D(2c) \geqq q'_D$. On the other hand, we have $q_D \leqq q'_D$ since q_D is the least split prime. Hence we get $q_D = q'_D$.

Second, we show this theorem when $d \equiv 1 \pmod 4$. Assume that x is odd, then $x^2 + d$ is even, hence we put $x^2 + d = 2q_D c$ ($c \geqq 1$). If c is divided by a split prime, then by the same way as $d \equiv 2 \pmod 4$, we get $q_D < \sqrt{d} = \sqrt{D/4}$.

Therefore $q_D > \sqrt{D/4}$ implies that $c = 1$ or the divisors of c are only ramified primes. Since x is odd, it holds $x^2 + d \equiv 2 \pmod 4$. Hence we have $4 \nmid (x^2 + d)$, and so c is odd. We get that an odd ramified prime divides c exactly by the same reason as $d \equiv 2 \pmod 4$. Hence we get $c \mid d$. Therefore we obtain $c \mid x$. Putting $x = cx_1$, we have $cx_1^2 + d/c = 2q_D$. Since $x_1 \geqq 1$, we have $q_D \geqq (c + d/c)/2 = q'_D(c) \geqq q'_D$. On the other hand, we have $q_D \leqq q'_D$. Thus we get $q_D = q'_D$. □

We conjecture that $q_D > \sqrt{D/4}$ implies $q_D = q'_D$ when $d \equiv 3 \pmod 4$, but we can not prove it yet. From Theorem 4.2 we have two corollaries as follows.

Corollary 4.3. *When* $d \equiv 2 \pmod 4$, *it holds that the conditions in Conjecture* 1.1 (i), (iv) *and* (v) *are equivalent.*

Proof. Theorem 3.4 says that $e_D \leqq 2$ implies $q_D > \sqrt{D} > \sqrt{D/4}$. And Theorem 4.2 says that $q_D > \sqrt{D/4}$ implies $q_D = q'_D$, On the other hand, $q_D = q'_D$ implies $q_D > \sqrt{D/3}$, because by $q_D = q'_D$ there is a divisor e of d such that $q_D = e + d/e$, hence $q_D = e + d/e > 2\sqrt{d} = \sqrt{D} > \sqrt{D/3}$. We have the property such that the ideal class group of K_D is generated by split ideals or ramified ideals which norms are less than $\sqrt{D/3}$. Therefore by $q_D > \sqrt{D/3}$ the ideal class group is generated by only ramified prime ideals, and so $\mathfrak{a}^2$ is principal for any ideal $\mathfrak{a}$ of K_D. Thus we obtain $e_D \leqq 2$. Hence we show that $q_D = q'_D$ implies $e_D \leqq 2$. Therefore (i), (iv) and (v) are equivalent. □

Corollary 4.4. *When $d \equiv 1 \pmod 4$, it holds that the conditions in Conjecture 1.1* (iv), (v) *and* (vi) *are equivalent.*

Proof. Shimizu [14] proved that $q_D = q'_D$ is equivalent to $f_D(x) = q_D^2$ for a integer x. Further we have that $q_D = q'_D$ implies $q_D > \sqrt{D/4}$, because by $q_D = q'_D$ there is a divisor e of d such that $q_D = (e + d/e)/2$, hence $q_D > \sqrt{d} = \sqrt{D/4}$. On the other hand we have proved that $q_D > \sqrt{D/4}$ implies $q_D = q'_D$ in Theorem 4.2. Therefore (iv), (v) and (vi) are equivalent. □

§ 5. Relations between prime-producing polynomials and $e_D \leqq 2$

In this section, we consider the inverse of Theorem 2.5, that is, whether it holds that EP-property implies $e_D \leqq 2$. But it does not hold when $d \equiv 1,\ 3 \pmod 4$. There are three counter examples with $d < 100,000,000$.

d	prime factors	d mod 4	h_D	t_D	2^{t_D-1}	p_D
2737	$7 \cdot 17 \cdot 23$	1	16	4	8	5
9867	$3 \cdot 11 \cdot 13 \cdot 23$	3	16	4	8	5
42427	$7 \cdot 11 \cdot 19 \cdot 29$	3	24	4	8	5

These imaginary quadratic fields satisfy EP-property, but do not satisfy $e_D \leqq 2$. On the other hand, when $d \equiv 2 \pmod 4$ we conjecture that EP-property implies $e_D \leqq 2$, and only when $t_D = 3$ we can prove it as below. Furthermore we generally conjecture that GEP-property implies $e_D \leqq 2$, but we can not prove it yet.

As we have described in Section 2, Rabinowitsch and Frobenius showed when $t_D = 1$ that EP-property holds if and only if $e_D \leqq 2$, and Hendy obtained the similar result when $t_D = 2$. From now on we consider the problem on EP-property when $t_D = 3$. We show the following theorem.

Theorem 5.1. *When $d = 2p_1p_2 \equiv 2 \pmod 4$ $(p_1 < p_2)$, the quadratic polynomial $2p_1x^2 + p_2$ takes prime values for all integers with $0 < x \leqq p_2 - 1$, then it holds $e_D \leqq 2$.*

For the proof of Theorem 5.1 we show the following lemma and theorem.

Lemma 5.2. *For any split prime q, there are integers x such that $q \mid f_{D,b}(x)$.*

Proof. There is an integer x_0 such that $q \mid f_D(x_0)$ by Lemma 3.2, then it holds $q \mid f_D(x_0 + yq)$ for every integer y.

When $d \equiv 2 \pmod 4$, we consider the equation $x_0 + yq = ax$, that is, $ax - qy = x_0$ in which x and y are integers. Since $\gcd(a,\ q) = 1$, there are solutions of this equation. Let $(x_1,\ y_1)$ be a solution, then we have $x_0 + y_1 q = ax_1$. Since $f_D(x_0 + y_1 q) = f_D(ax_1) = a(ax_1^2 + b)$, we obtain $q \mid a(ax_1^2 + b)$, and so $q \mid (ax_1^2 + b)$. Hence we have $q \mid f_{D,b}(x_1)$.

When $d \equiv 1 \pmod 4$, we consider $x_0 + yq = 2ax + a$. Since $\gcd(2a,\ q) = 1$, there are solutions of this equation. Let $(x_1,\ y_1)$ be a solution, then we have $x_0 + y_1 q = 2ax_1 + a$. Since $f_D(x_0 + y_1 q) = f_D(2ax_1 + a) = 2a\{2ax_1^2 + 2ax_1 + (a+b)/2\}$, we obtain $q \mid 2a\{2ax_1^2 + 2ax_1 + (a+b)/2\}$, and so $q \mid \{2ax_1^2 + 2ax_1 + (a+b)/2\}$. Hence we have $q \mid f_{D,b}(x_1)$.

When $d \equiv 3 \pmod 4$, we consider $x_0 + yq = ax + (a-1)/2$. Since $\gcd(a,\ q) = 1$, there are solutions of this equation. Let $(x_1,\ y_1)$ be a solution, then we have $x_0 + y_1 q = ax_1 + (a-1)/2$. Since $f_D(x_0 + y_1 q) = f_D(ax_1 + (a-1)/2) = a\{ax_1^2 + ax_1 + (a+b)/4\}$, we obtain $q \mid \{ax_1^2 + ax_1 + (a+b)/4\}$. Hence we have $q \mid f_{D,b}(x_1)$. □

Using Lemma 5.2 we prove the following.

Theorem 5.3. *Suppose $d \equiv 2 \pmod 4$. Let b be the largest prime divisor of d and $a{=}d/b$. We assume $b > \sqrt{D/16}$. If the quadratic polynomial $f_{D,b}(x)$ takes prime values for all integers x with I_b, then it holds $e_D \leqq 2$.*

Proof. In this case, we have $f_{D,b}(x) = ax^2 + b$ and $I_b = \{x \mid 0 < x \leqq b - 1\}$. From Lemma 5.2, there are integers x such that $q_D \mid (ax^2 + b)$. Suppose that x_1 is the least positive integer such x.

If $0 < x_1 \leqq b - 1$, namely, $x \in I_b$, then by Lemma 3.3 we have that $ax_1^2 + b$ is a split prime. Since q_D is the least split prime, we get $q_D = f_{D,b}(1)$, thus

$$q_D = a + b > 2\sqrt{d} > \sqrt{D/4}.$$

Now suppose $x_1 \geqq b$. Since x_1 is the least positive integer such that $q_D \mid (ax^2 + b)$, we have $q_D/2 > x_1$. By $x_1 \geqq b$, we have $q_D/2 > b$. Since $b > \sqrt{D/16}$ we get $q_D/2 > \sqrt{D/16}$, namely, $q_D > \sqrt{D/4}$.

Therefore we obtain $e_D \leqq 2$ by Corollary 4.3. □

Using Theorem 5.3 we prove Theorem 5.1.

Proof. (Theorem 5.1) Let $a = 2p_1$ and $b = p_2$, then we have $f_{D,b}(x) = 2p_1 x^2 + p_2$ and $I_b = \{x \mid 0 < x \leqq p_2 - 1\}$. In this case the condition $b > \sqrt{D/16}$ holds. Thus we complete the proof. □

Theorem 5.4. *When* $d \equiv 2 \pmod 4$ *and* $t_D = 3$, *it holds that the conditions in Conjecture* 1.1 (i), (ii), (iii), (iii)$'$, (iv) *and* (v) *are equivalent.*

Proof. We have already shown that (i), (iv) and (v) are equivalent in Corollary 4.3. Further by Theorem 5.1 EP-property implies $e_D \leqq 2$ when $t_D = 3$. On the other hand, it holds that $e_D \leqq 2$ implies $p_D = t_D$ and that $p_D = t_D$ implies EP-property by Mollin [6][7][8]. Furthermore by Theorem 3.1 $e_D \leqq 2$ implies GEP-property, and it is trivial that GEP-property implies EP-property. Thus we complete the proof. □

X.Guo and H.Qin [3] showed under the Extended Riemann Hypothesis that $e_D \leqq 2$ is equivalent to $p_D = 3$ when $t_D = 3$. By Theorem 5.4 we have obtained without the Extended Riemann Hypothesis that $e_D \leqq 2$ is equivalent to $p_D = 3$ and $t_D = 3$ when $d \equiv 2 \pmod 4$.

§ 6. Relations between prime-producing polynomials and $q_D > \sqrt{D/4}$

We want to prove that EP-property implies $e_D \leqq 2$ when $t_D = 3$ and $d \equiv 1 \pmod 4$, too. But we cannot prove it yet. In this section we show that EP-property implies $q_D > \sqrt{D/4}$ when $t_D = 3$ and $d \equiv 1 \pmod 4$. We prove the following theorem.

Theorem 6.1. *Suppose* $d = p_1 p_2 \equiv 1 \pmod 4$ $(p_1 < p_2)$. *If the quadratic polynomial* $2p_1x^2 + 2p_1x + (p_1 + p_2)/2$ *takes prime values for all integers with* $0 \leqq x \leqq p_2/2 - 1$, *then it holds* $q_D > \sqrt{D/4}$.

For the proof of Theorem 6.1 we show the following.

Theorem 6.2. *Suppose* $d \equiv 1 \pmod 4$. *Let* b *be the largest prime divisor of* d *and* $a = d/b$. *We assume* $b > \sqrt{D/4}$. *If the quadratic polynomial* $f_{D,b}(x)$ *takes prime values for all integers* x *with* I_b, *then it holds* $q_D > \sqrt{D/4}$.

Proof. In this case, we have $f_{D,b}(x) = 2ax^2 + 2ax + (a+b)/2$ and $I_b = \{x \mid 0 \leqq x \leqq b/2 - 1\}$. From Lemma 5.2, there are integers x such that $q_D \mid \{2ax^2 + 2ax + (a+b)/2\}$. Suppose that x_1 is the least non-negative integer such x.

If $0 \leqq x_1 \leqq b/2 - 1$, namely, $x_1 \in I_b$, then we have that $f_{D,b}(x) = 2ax_1^2 + 2ax_1 + (a+b)/2$ is a split prime. Since q_D is the least split prime, we get $q_D = f_{D,b}(0)$. Hence we have

$$q_D = (a+b)/2 > \sqrt{d} = \sqrt{D/4}.$$

Next, suppose $x_1 > b/2-1$. Since $(q_D-1)/2 > x_1$, we have $(q_D-1)/2 > b/2-1$, and so $q_D \geqq b$. By $b > \sqrt{D/4}$, we have $q_D > \sqrt{D/4}$. Thus we complete the proof. $\square$

From Theorem 6.2 we have the proof of Theorem 6.1.

Proof. (Theorem 6.1) Let $a = p_1$ and $b = p_2$, then we have $f_{D,b}(x) = 2p_1x^2 + 2p_1x+(p_1+p_2)/2$ and $I_b = \{x \mid 0 \leqq x \leqq p_2/2-1\}$. In this case, the condition $b > \sqrt{D/4}$ holds. Thus from Theorem 6.2 we complete the proof. $\square$

Theorem 6.3. *When* $d \equiv 1 \pmod 4$ *and* $t_D = 3$, *we have the following relations between conditions in Conjecture* 1.1.

$$\begin{array}{ccccc} (\mathrm{i}) & \Rightarrow & (\mathrm{ii}) & \Rightarrow & (\mathrm{iii})' \\ & & & & \Downarrow \\ & & (\mathrm{iv}) & \Leftrightarrow & (\mathrm{v}) \Leftrightarrow (\mathrm{vi}) \end{array}$$

Proof. Theorem 2.4 and 2.5 say that (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii)$'$, and Theorem 6.1 says that (iii)$'$ $\Rightarrow$ (v) when $t_D = 3$. Further the equivalence between (iv), (v) and (vi) is given by Corollary 4.4. Thus we complete the proof. $\square$

Acknowledgment

The author would like to thanks the referee for his valuable comments and suggestions.

References

[1] F. G. Frobenius: Über quadratische Formen, die viele Primzahlen darstellen, Sitzungsber. d. Königl. Akad. d. Wiss. zu Berlin, 966-980 (1912)
[2] H. Gu, D. Gu and Y. Liu : Ono invariants of imaginary quadratic fields with class number three, J. Number Theory **127**, 262-271 (2007)
[3] X. Guo and H. Qin : Imaginary quadratic fields with Ono number 3, Comm. in Algebra, Vol.38, Issue 1, 230-232 (2010)
[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 von Rabinowitsch über imaginär-quadratische Zahlkörper, J. Reine Angew. Math. **285**, 100-113 (1976).
[6] R. A. Mollin : Orders in quadratic fields III, Proc. Japan Acad. **70A**, 176-181 (1994).

[7] R. A. Mollin : Quadratics, CRC Press, Boca Raton (1995).
[8] R. A. Mollin : A completely general Rabinowitsch criterion for complex quadratic fields, Canad. Math. Vol. **39**(1), 106-110 (1996).
[9] T. Ono : Arithmetic of algebraic groups and its applications, St. Paul's International Exchange Series Occasional Papers VI, St. Paul's University, Tokyo (1986).
[10] G. Rabinowitsch : Eindeutigkeit der Zerlegung in Primzahlfaktoren in quadratischen Zahlkörpern, J. Reine Angew. Math. **142**, 153-164 (1913).
[11] F. Sairaiji and K. Shimizu : A note on Ono's numbers associated to imaginary quadratic fields, Proc. Japan Acad. **77A**, 29-31 (2001).
[12] 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).
[13] R. Sasaki : On a lower bound for the class number of an imaginary quadratic field, Proc. Japan Acad. **62A**, 37-39 (1986).
[14] K. Shimizu: Imaginary quadratic fields whose exponents are less than or equal to two, Math. J. Okayama Univ. Vol. 50, 85-99 (2008)