R. A. Mollin and H. C. Williams
Nagoya Math. J.
Vol. 112 (1988), 143-151

ON PRIME VALUED POLYNOMIALS AND CLASS NUMBERS OF REAL QUADRATIC FIELDS

R.A. MOLLIN AND H.C. WILLIAMS

§1. Introduction

Gauss conjectured that there are infinitely many real quadratic fields with class number one. Today this is still an open problem. Moreover, as Dorian Goldfeld, one of the recipients of the 1987 Cole prize in number theory (for his work on another problem going back to Gauss) recently stated in his acceptance of the award: "This problem appears quite intractible at the moment." However there has recently been a search for conditions which are tantamount to class number one for real quadratic fields. This may be viewed as an effort to shift the focus of the problem in order to understand more clearly the inherent difficulties, and to reveal some other beautiful interrelationships.

One of the avenues of inquiry has been to search for criteria in terms of prime valued polynomials. The impetus for this search has come from a result for complex quadratic fields which is almost 75 years old.

THEOREM 1.1 (Rabinowitsch [13] and [14]). *If* $d \equiv 3 \pmod 4$ *where* d *is a positive square-free integer, then* $p(x) = x^2 - x + (d+1)/4$ *is prime for all integers* x *with* $1 \leq x \leq (d-3)/4$ *if and only if* $h(-d) = 1$.

It is now well-known (see [2], [5], and [17]) that there exactly nine complex quadratic fields with class number one. They are $Q(\sqrt{-d})$ for $d \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}$. Thus together with Theorem 1.1 we get the remarkable:

THEOREM 1.2. *If* $d \equiv 3 \pmod 4$ *is a square-free integer then* $x^2 - x + (d+1)/4$ *is prime for all integers* x *with* $1 \leq x \leq (d-3)/4$ *if and only if* $d \in \{7, 11, 19, 43, 67, 163\}$.

Given Gauss' open conjecture cited at the outset, the story for real

Received May 25, 1987.

quadratic fields and prime quadratics is not so neat. However recent headway has been made and we will now detail this history culminating in the criteria which we have discovered.

In [6] Kutsuna found a necessary and sufficient condition for an arbitrary real quadratic field to have class number one. However the condition involves so-called störend fractions and is nearly impossible to apply in practice. However a consequence of his result is more readily applied and is more pertinent.

PROPOSITION 1.1 (Kutsuna [6]).

(a) *Let* $d = 1 + 4m$ *be square-free positive integer. If* $-x^2 + x + m$ *is prime for all integers* x *with* $1 \leq x \leq \sqrt{m} - 1$ *then* $h(d) = 1$.

(b) *If* m *is odd and* $(d/p) = -1$ *for every prime* p *with* $2 < p \leq \sqrt{m}$ *then* $h(d) = 1$. *(Here* $(*/*)$ *denotes the Legendre symbol.)*

At this juncture we digress to introduce a conjecture of S. Chowla [3], since this is the point of entry of the authors' work on the problem. S. Chowla conjectured that if $d = \ell^2 + 1$ is prime and $\ell > 26$ then $h(d) > 1$. Proposition 1.1 is unsatisfactory in this regard since it fails to be of value when m is a square. However with Kutsuna's result as an inspiration, Mollin [8] achieved the following result:

THEOREM 1.3. *Let* $d = 4m^2 + 1$ *be square-free and positive where* m *is a positive integer. Then the following are equivalent.*

(1) $h(d) = 1$;

(2) p *is inert in* $Q(\sqrt{d})$ *for all primes* $p < m$;

(3) $f_d(x) = -x^2 + x + m^2 \not\equiv 0 \pmod{p}$ *for all positive integers* x *and primes* p *satisfying* $x < p < m$;

(4) $f_d(x)$ *is prime for all integers* x *with* $1 < x < m$.

These conditions are certainly quite strong, yet the Chowla conjecture remains open. However Mollin and Williams [12] were able to use Theorem 1.3 together with the generalized Riemann hypothesis (G.R.H.) to prove it.

A similar conjecture for $d = m^2 + 4$ was made by Yokoi [18] wherein he conjectured that if $m > 17$ is prime then $h(d) > 1$. Moreover in [9], Mollin conjectured that for square-free $d = m^2 - 4$ with $m > 21$ then $h(d) > 1$. We establish all three conjectures (modulo G.R.H.) in Section 2.

The results of this paper generalize, improve or contain as special cases certain results of Azuhata [1], Louboutin [7], Mollin [9], Mollin and Williams [12], Sasaki [16], and Yokoi [18].

§ 2. Results

With the work on the Chowla conjecture (see § 1) as a stepping stone we shift attention to the more general question of obtaining class number one criteria for arbitrary real quadratic fields. We begin with a very general result which is stated separately since it is of interest in its own right.

For the remainder of the paper we set:

$$f_d(x) = \begin{cases} -x^2 + x + (d-1)/4 & \text{if } d \equiv 1 \pmod 4 \\ -x^2 + d & \text{if } d \not\equiv 1 \pmod 4 \end{cases}$$

where d is a square-free integer.

LEMMA 2.1. *If α is any positive real number then the following are equivalent.*

(1) *p is inert in $Q(\sqrt{d})$ for all primes $p < \alpha$; i.e., $(d/p) = -1$ for all odd primes $p < \alpha$ and $d \equiv 5 \pmod 8$ for $2 < \alpha$.*

(2) *$f_d(x) \not\equiv 0 \pmod p$ for all integers x and primes p such that $0 \leq x < p < \alpha$.*

Proof. First we assume that (1) holds. Suppose that $f_d(x) \equiv 0 \pmod p$ for some prime p and integer x with $0 \leq x < p < \alpha$. Therefore, if $p > 2$ then:

$$d \equiv \begin{cases} (2x-1)^2 \pmod p & \text{if } d \equiv 1 \pmod 4 \\ x^2 \pmod p & \text{if } d \not\equiv 1 \pmod 4 \end{cases}$$

whence p is not inert in $Q(\sqrt{d})$. If $p = 2$ then $x \in \{0, 1\}$, whence $d \not\equiv 5 \pmod 8$; i.e., $p = 2$ is not inert in $Q(\sqrt{d})$. Thus (1) implies (2).

Conversely assume that (2) holds and that there is a prime $p < \alpha$ such that p is not inert in $Q(\sqrt{d})$. Therefore if $p > 2$ there is an integer x such that:

$$d \equiv \begin{cases} (2x-1)^2 \pmod p & \text{with } 0 < x \leq (p+1)/2 & \text{if } d \equiv 1 \pmod 4 \\ x^2 \pmod p & \text{with } 0 \leq x < p & \text{if } d \not\equiv 1 \pmod p . \end{cases}$$

Hence $f_d(x) \equiv 0 \pmod{p}$ for some integer x and prime p with $0 \leqslant x < p < \alpha$. This contradicts (2). If $p = 2$ and $d \equiv 1 \pmod 4$, then $f_d(0) \equiv f_d(1) = (d-1)/4 \not\equiv 0 \pmod 2$: i.e., $d \equiv 5 \pmod 8$ contradicting that p is not inert. Therefore $d \not\equiv 1 \pmod 4$, $f_d(0) = d \not\equiv 0 \pmod 2$, and $f_d(1) = d - 1 \not\equiv 0 \pmod 2$, a contradiction. This establishes the result. Q.E.D.

Now we particularize a situation more germane to the central theme. For the remainder of the paper we set:

$$\alpha = \begin{cases} (\sqrt{d-1})/2 & \text{if } d \equiv 1 \pmod 4 \\ \sqrt{d} & \text{if } d \not\equiv 1 \pmod 4 . \end{cases}$$

Moreover since we will have occasion to refer to the following statements several times throughout the balance of the paper we label them once and for all at this juncture as:

CONDITIONS.

(I) p is inert in $Q(\sqrt{d})$ for all primes $p < \alpha$;

(II) $f_d(x) \not\equiv 0 \pmod p$ for all integers x and primes p such that $0 \leq x < p < \alpha$;

(III) $f_d(x)$ is a prime for all integers x with $1 < x < \alpha$;

(IV) $h(d) = 1$.

LEMMA 2.2. (I) $\Leftrightarrow$ (II) $\Rightarrow$ (III) $\Rightarrow$ (IV). *Additionally if* $d \equiv 1 \pmod 4$ *then* (III) $\Rightarrow$ (II).

Proof. The equivalence of (1) and (II) is a special case of Lemma 2.1. Now we show that (II) implies (III).

Suppose that $f_d(x)$ is composite for some integer x with $1 < x < \alpha$. If all primes dividing $f_d(x)$ are larger than or equal to α then $f_d(x) \geq \alpha^2$, whence $x \leq 1$, a contradiction. Hence there exists a prime divisor p of $f_d(x)$ such that $p < \alpha$. If p also divides x then $f_d(0) \equiv 0 \pmod p$. This contradicts (II). Therefore p does not divide x and so we may assume $f_d(x) \equiv 0 \pmod p$ for some integer x with $0 < x < p < \alpha$, contradicting (II).

Next we show that when $d \equiv 1 \pmod 4$ then (III) implies (II), whence (I) $\Leftrightarrow$ (II) $\Leftrightarrow$ (III). Assume (III) holds and $f_d(x) \equiv 0 \pmod p$ for some integer x and prime p with $0 \leq x < p < \alpha$. If $x > 1$ then $f_d(x) = p$ from (III). However, $x < \alpha$ implies that $x(1-x) > \alpha(1-\alpha)$, whence $f_d(x) = p > \alpha$, a contradiction. Hence $x \in \{0, 1\}$, whence p divides α^2. Therefore $f_d(p) = p(-p + 1 + \alpha^2/p)$. By (III) $f_d(p) = p$, where $p = \alpha$, a contradiction.

Finally assume (III) holds, and suppose $h(d) > 1$. If $d \not\equiv 1 \pmod 4$ then $d \leq 11$ is forced and the result holds. Therefore assume $d \equiv 1 \pmod 4$. Thus by Kutsuna [6, Propositions 3 and 4, p. 126] we have that there exists an integer a and a prime p such that $0 \leq a < p \leq \alpha$ and both:

(a) $N(a - \beta) \equiv 0 \pmod p$ where $\beta = (1 + \sqrt{d})/2$;

and

(b) There does not exist an integer k such that $|N(a + kp - \beta)| < p^2$, where N is the absolute norm.

From (a) it follows that $f_d(a) \equiv 0 \pmod p$. If $a > 1$ then (III) implies that $f_d(a) = p$. However setting $k = 0$ in (b) yields that $f_d(a) \geq p^2$ a contradiction. Hence $a \in \{0, 1\}$, and so p divides α^2, whence $f_d(p) = p(-p + 1 + \alpha^2/p)$. From (III) it follows that $\alpha = p$. If $k = 1$ in (b) then $p^2 \leq |N(a + p - \beta)| = p$, a contradiction.

Table 2.1. $h(d) = 1$.

d	prime values of $f_d(x)$ for $1 < x < \alpha$
2	–
3	–
5	–
6	2
7	3
11	2, 7
13	11
17	–
21	3
29	5
37	7
53	7, 11
77	7, 13, 17
101	13, 19, 23
173	13, 23, 31, 37, 41
197	19, 29, 37, 43, 47
293	17, 31, 43, 53, 61, 67, 71
437	19, 37, 53, 67, 79, 83, 97, 103, 107
677	37, 59, 79, 97, 113, 127, 139, 149, 157, 163, 167.

We conjecture that the entries in Table 2.1 represent *all* of those d for which $f_d(x)$ is prime with $1 < x < \alpha$. We will establish this conjecture (modulo G.R.H.) at the end of the paper. First we observe that the

entries $d > 13$ in Table 2.1 share a common property. They are of *narrow Richaud-Degert* (R-D) type (see [4], [10] and [15]); i.e., $d = m^2 + r \neq 5, 13$ where $|r| \in \{1, 4\}$. This is not an accident. In point of fact it tells the whole story, as we shall see.

LEMMA 2.3. *If* (III) *holds for* $d > 13$ *then* $d \equiv 1 \pmod 4$ *and* d *is of narrow R-D type.*

Proof. If $d \not\equiv 1 \pmod 4$ then for $d > 6$, $f_d(2)$ is even composite when $d \equiv 2 \pmod 4$, and for $d > 13$, $f_d(3)$ is even composite when $d \equiv 3 \pmod 4$. Hence $d \equiv 1 \pmod 4$. By Lemma 2.2 (III) $\Rightarrow$ (I), whence $d \equiv 5 \pmod 8$ when $d > 17$. Since 17 is of narrow R-D type we assume henceforth that $d \equiv 5 \pmod 8$.

Set $d = m^2 + t$ where $0 < t < 2m$. If t is divisible by two odd primes p and q then by Lemma 2.2 (III) $\Rightarrow$ (I) we must have that $t \geq pq \geq (d - 1)/4$ since neither p nor q is inert in $Q(\sqrt{d})$. Therefore $d = m^2 + t \geq m^2 + (d - 1)/4$. Since $t < 2m$ then $m^2 + 2m > m^2 + (d - 1)/4$; i.e., $m^2 - 8m + t - 1 < 0$. However $t \geq 15$ since it is divisible by two odd primes; whence $m^2 - 8m + 14 < 0$, a contradiction. We may now assume that $t = 2^a p^b$ for $a \in \{0, 2\}$ and $b \in \{0, 1\}$, when p is an odd prime. If $b = 0$ then d is of narrow R-D type so we assume that $t = 4p$ or $t = p$. If $t = 4p$ then $p < m/2$. If $m/2 < (\sqrt{d - 1})/2$ then (I) is contradicted. Hence $m \geq \sqrt{d - 1}$; i.e., $m^2 \geq m^2 + 4p - 1$, a contradiction; whence $t = p$. Set $d = (m + 1)^2 - (2m + 1 - p) = (m + 1)^2 - s$, say. If s is divisible by two odd primes then $s \geq (d - 1)/4$ by (I) again. Therefore $d = (m + 1)^2 - s \leq (m + 1)^2 - (d - 1)/4$; i.e., $(5d - 1)/4 \leq (m + 1)^2$. Thus, $5(m + 1)^2 - 5s - 1 \leq 4(m + 1)^2$; i.e., $(m + 1)^2 - 5s - 1 \leq 0$. However $s < 2m$, therefore $(m + 1)^2 - 10m - 1 < 0$, whence $m \leq 7$. The only solution to $13 < d = m^2 + p$ for $m \leq 7$ and $p < 2m$ is $d = 21$ which is of narrow R-D type. Hence $s = 2^e q^f$ where $e \in \{0, 2\}$, $f \in \{0, 1\}$, and q is an odd prime. If $f = 0$ then d is of narrow R-D type. Thus we assume that $s = 4q$ or $s = q$. If $s = 4q$ then $q < m/2$, since $s < 2m$. By (I), $q \geq (\sqrt{d - 1})/2$, whence $m > \sqrt{d - 1}$; i.e., $m^2 > m^2 + p - 1$, a contradiction. Therefore $s = q$; i.e., $2m + 1 = p + q \equiv 0 \pmod 2$, a contradiction. This completes the proof.

THEOREM 2.1. *Let* $d > 13$ *then* (I) $\Leftrightarrow$ (II) $\Leftrightarrow$ (III) $\Leftrightarrow$ (IV) *holds if and only if* $d \equiv 1 \pmod 4$ *and* d *is of narrow R-D type.*

Proof. If $d \equiv 1 \pmod 4$ and d is of narrow R-D type then by Mollin

[9] the result follows.

Conversely if (I) $\Leftrightarrow$ (II) $\Leftrightarrow$ (III) $\Leftrightarrow$ (IV) then the result follows from Lemma 2.3.

COROLLARY 2.1. *$h(d) > 1$ if any of the following conditions hold:*

(1) *$d = m^2 + 1$ with $m > 1$ odd;*

(2) *$d = m^2 - 1$ with $m > 2$ even;*

(3) *$d = 4m^2 + 1$ with m composite;*

(4) *$d = m^2 \pm 4$ with $(d - 1)/4$ composite.*

Corollary 2.1 was also obtained from results for non-trivial class numbers by Mollin in [10]–[11]. We also observe that Corollary 2.1 reduces the aforementioned Chowla conjecture to the case where $d = 4p^2 + 1$, $p > 2$ prime, and the aforementioned Yokoi conjecture to the case where $d = m^2 + 4 = 4p + 1$, p a prime. Furthermore the aforementioned Mollin conjecture reduces to $h(d) = 1$ for square-free $d = m^2 - 4$ if and only if $d \in \{5, 21, 77, 437\}$. We now establish all of these conjectures subject to G.R.H.

THEOREM 2.2. *If G.R.H. holds and $d > 13$ then* (I) $\Leftrightarrow$ (II) $\Leftrightarrow$ (III) $\Leftrightarrow$ (IV) *holds if and only if d is an entry in Table* 2.1.

Proof. By employing the same argument as that used in [12], we see that when d is a square-free positive integer and $d \equiv 1 \pmod 4$ we get $h(d) > \sqrt{d}\, e^{-t(d)}/2(\log d)^2 R$ where R is the regulator of $Q(\sqrt{d})$ and;

$$t(x) = (3/\pi) + (15.9/2 \log\log x) + (2/\pi \log\log x) + (5.3/(\log\log x)^2) + (8/\log x \log\log x) + (6 \log\log x/\pi \log x) + (12/\log x) + (4/\pi \log x) + (1/(\log x)^2)\,.$$

If $5 < d = m^2 \pm 4 \equiv 5 \pmod 8$ then the fundamental unit of $Q(\sqrt{d})$ is $(m + \sqrt{d})/2$ and $R = \log((m + \sqrt{d})/2) < \log(\sqrt{d} + 1)$. If we put:

$$F(d) = \sqrt{d}\, e^{-t(d)}/(2(\log d)^2 \log(\sqrt{d} + 1))$$

then we have $h(d) > F(d)$. Moreover $F(d)$ is an increasing function of d. When $d = 10^{13}$, we have $F(d) > 1$; hence, $h(d) > 1$ for any square-free $d \geq 10^{13}$. It remains to deal with the case of $d < 10^{13}$.

From a result of Mollin [9, Corollary 3] it is easy to see that if $d = m^2 \pm 4$ then $h(d) > 1$ whenever there exists some prime q such that $q < m - 2$ and q is not inert in $Q(\sqrt{d})$. Since m must be odd we write

it as $2s + 1$ and consider the values of d of the form $g_1(s) = 4s^2 + 4s - 3$ and $g_2(s) = 4s^2 + 4s + 5$. Since $d < 10^{13}$, we have $s < 1.6 \times 10^6$. For a fixed $g_n(s)$ $(n \in \{1, 2\})$ we select a positive integer k and the first k odd primes $\{q_i\}_{i=1}^k$. For each of these q_i we tabulate those S_{ij} such that $0 \leq S_{ij} \leq q_i - 1$ and $(g_n(S_{ij})/q_i) = 1$. If any $s \equiv S_{ij} \pmod{q}$ and $2s - 1 > q_i$, then the value of $d = g_n(s)$ must have $h(d) > 1$. Hence this value of s can be deleted from the 1.6×10^6 to be considered. We used a value of $k = 30$ and a Fortran program to eliminate all the possible candidates for s, except $s = 1, 2, 4, 5, 10$ when $n = 1$ and $s = 1, 2, 3, 5, 6, 8$ when $n = 2$. The computer was able to sieve out all the other values in a little less than 20 seconds for each $g_n(s)$ form. Hence, if $s > 10$ and the G.R.H. holds, we must have $h(d) > 1$. This establishes the result.

COROLLARY 2.2. *If G.R.H. holds then* (III) $\Leftrightarrow$ (IV) *if and only if* d *is an entry in Table* 2.1; *i.e., if G.R.H. holds then Table* 2.1 *contains all R-D types of class number one.*

Thus we have proved the following real analog of Theorem 1.2.

THEOREM 2.8. *If G.R.H. holds then* $f_d(x)$ *is prime for all integers* x *with* $1 < x < \alpha$ *if and only if* d *is entry in Table* 2.1.

REFERENCES

[1] T. Azuhata, On the fundamental units and the class numbers of real quadratic fields, Nagoya Math. J., **95** (1984), 125–135.
[2] A. Baker, Linear forms in the logarithms of algebraic numbers, Mathematika, **13** (1966), 204–216.
[3] S. Chowla and J. Friedlander, Class numbers and quadratic residues, Glasgow Math. J., **17** (1976), 47–52.
[4] G. Degert, Uber die bestimmung der grundeinheit gewisser reellquadratischen zahlkorper, Abh. Math. Sem. Univ. Hamburg, **22** (1958), 92–97.
[5] D. Goldfeld, Gauss' class number problems for imaginary quadratic fields, Bull. Amer. Math. Soc., **13** (1985), 23–37.
[6] M. Kutsuna, On a criterion for the class number of a quadratic number field to be one, Nagoya Math. J., **79** (1980), 123–129.
[7] S. Louboutin, Critères des principalité et minoration des nombres de classes l'ideaux des corps quadratiques réells à l'aide de la théorie des fractions continues, preprint.
[8] R. A. Mollin, Necessary and sufficient conditions for the class number of a real quadratic field to be one, and a conjecture of S. Chowla, Proceedings Amer. Math. Soc., **102** (1988), 17–21.
[9] ——, Class number one criteria for real quadratic fields I, Proceedings Japan Acad., Series A, **83** (1987), 121–125.
[10] ——, On the insolubility of a class of diophantine equations and the nontriviality

of the class numbers of related real quadratic fields of Richaud-Degert type, Nagoya Math. J., **105** (1987), 39–47.

[11] ——, Diophantine equations and class numbers, J. Number Theory, **24** (1986), 7–19.

[12] R. A. Mollin and H. C. Williams, A conjecture of S. Chowla via the generalized Riemann hypothesis, Proceedings Amer. Math. Soc., **102** (1988), 794–796.

[13] G. Rabinowitsch, Eindentigkeit der zerlegung in primzahlfaktoren in quadratischen zahlkörpern, Proc. Fifth Internat. Congress Math. (Cambridge) Vol. **1** (1913), 418–421.

[14] ——, Eindeutigkeit der zerlegung in primzahlfaktoren in quadratischen zahlkörpern, J. reine angew. Math., **142** (1913), 153–164.

[15] C. Richaud, Sur la résolution des équations $x^2 - Ay^2 = \pm 1$, Atti. Acad. Pontif. Nuovi. Lincei (1866), 177–182.

[16] R. Sasaki, Generalized ono invariant and Rabinovitch's theorem for real quadratic fields, preprint.

[17] H. Stark, A complete determination of the complex quadratic fields of class-number one, Michigan Math. J., **14** (1967), 1–27.

[18] H. Yokoi, Class-number one problem for certain kind of real quadratic fields, Proc. Int. Conf. on class numbers and fundamental units, June 1986, Katata Japan, 125–137.

R. A. Mollin
Department of Mathematics and Statistics
University of Calgary
Calgary, Alberta
Canada T2N 1N4

H. C. Williams
Department of Computer Science
University of Manitoba
Winnipeg, Manitoba
Canada R3T 2N2