ACTA ARITHMETICA
LXXXIX.1 (1999)

Prime producing polynomials: Proof of a conjecture by Mollin and Williams

by

ANITHA SRINIVASAN (Humacao, P.R.)

1. Introduction. At the 1912 International Congress of Mathematicians, Rabinowitsch showed that n^2+n+A is prime for $n=0,1,\ldots,A-2$ if and only if $-d:=4A-1$ is squarefree and $h(d)=1$ (where $h(d)$ is the class number of the quadratic field $\mathbb{Q}(\sqrt{d})$). Recent research (see [Mo]) has focussed on giving similar criteria for real quadratic fields, which tend to be complicated by the existence of infinitely many units in the field. The prototype is the following result of Mollin and Williams (see [Mo, pp. 352–354]): $A-n-n^2$ is prime for all positive $n<\sqrt{A}-1$ if and only if $d:=4A+1$ is squarefree, $h(d)=1$, and either $d=17$, or $d\ge 21$ with $d\equiv 5 \bmod 8$, where d is of the form $4m^2+1$ or $m^2\pm 4$, for some integer m.

Subsequently there have been many investigations of prime producing polynomials and their connection to the structure of real quadratic fields, as discussed in Mollin's delightful book [Mo]. Included there is the following conjecture of Mollin and Williams (see page 140, Conjecture 4.2.1 in [Mo]):

THE MOLLIN–WILLIAMS CONJECTURE. *Let $d=pq\equiv 5 \bmod 8$, where $p<q$ are primes congruent to $3 \bmod 4$. Then the following are equivalent.*

(i) *$|pk^2+pk+(p-q)/4|$ is prime or equal to 1 whenever $0\le k\le \sqrt{d}/4-1/2$.*

(ii) *The class number $h(d)$ is 1 and $d=p^2s^2\pm 4p$ or $d=4p^2s^2-p$.*

The main result in this paper is

THEOREM 1. *Suppose that $d=pq\equiv 5 \bmod 8$, where $p<q$ are primes congruent to $3 \bmod 4$, and that $|pk^2+pk+(p-q)/4|$ is prime or equal to 1 whenever $0\le k\le \sqrt{d}/4-1/2$. Then the class number $h(d)$ is 1 and the length $l(d)$ of the principal cycle does not exceed 10.*

1991 *Mathematics Subject Classification*: 11R09, 11R29, 11E16.

Key words and phrases: class number, binary quadratic forms, prime producing polynomials.

As we will now explain, this implies

Corollary. *The Mollin–Williams conjecture holds for all, except perhaps one, integer d of the form $d = pq \equiv 5 \bmod 8$, where $p < q$ are primes congruent to* $3 \bmod 4$. *If this exceptional d exists then* (ii) *would hold but not* (i), *and it would mean that $L(s,(d/\cdot))$ has a zero far to the right of the half-line—that is, the Riemann Hypothesis would be false for this L-function.*

To deduce the Corollary from Theorem 1, we use computational results of Mollin and Williams [MW]. They found, with at most one possible exception, the complete (finite) list of all positive discriminants of class number 1, which have less than 25 forms in their principal class. Putting aside the possible exception, their list thus contains all the d that arise from Theorem 1. Moreover discriminants d of the form $d = p^2s^2 \pm 4p$ or $d = 4p^2s^2 - p$ have either 2 or 4 forms in the principal class, and so Mollin and Williams's list contains all the d that satisfy statement (ii), with that one possible exception. Examining their data one can compile the list of discriminants therein and verify the conjecture for these d:

Proposition. *All* $d \in \{21, 69, 77, 93, 141, 213, 237, 413, 437, 453, 573, 717, 1077, 1133, 1253, 1293, 1757\}$ *satisfy* $h(d) = 1$, *can be written in the form $d = pq \equiv 5 \bmod 8$, where $p < q$ are primes congruent to* $3 \bmod 4$, *and can be written in the form $d = p^2s^2 \pm 4p$ or $d = 4p^2s^2 - p$ for some integer s. Moreover $|pk^2 + pk + (p-q)/4|$ is prime or equal to* 1 *whenever* $0 \le k \le \sqrt{d}/4 - 1/2$.

The one possible exceptional d would have to have a particularly small value for $L(1,(d/\cdot))$—Mollin and Williams's proof uses the lower bound for $L(1,(d/\cdot))$ given by Tatuzawa as a modification of an argument of Siegel—and thus $L(s,(d/\cdot))$ would contradict the Generalized Riemann Hypothesis.

Therefore the Corollary follows from the computations of Mollin and Williams, once one has shown that (i) implies (ii) (or something slightly weaker). Previous work on this subject by Louboutin works only when we extend the range of the hypothesis in (i): Louboutin [L1, Theorem 9] proved that (i) implies (ii), with no exceptions, when the range for k is allowed to go up to $\sqrt{d}/2 - 1/2$. In [L1, L2] he proved that if the range for k is allowed to go up to $\sqrt{d}/3 - 1/2$ then either (ii) in the conjecture holds or $d = p((3b+4)^2+4)/9$ with $p \equiv -1 \bmod 12$ (and, in the latter case, there is at most one such d with $h(d) = 1$, according to the aforementioned Siegel–Tatuzawa bound).

Our proof begins by showing that if Q is a prime $< \sqrt{d}/2$, then Q is non-inert if and only if Q divides $|pk^2 + pk + (p-q)/4|$ for some k in $[0, \sqrt{d}/4 - 1/2]$. Since none of these numbers are composite by hypothesis, every non-inert prime less than $\sqrt{d}/2$ is of the form $|pk^2 + pk + (p-q)/4|$

for k in $[0, \sqrt{d}/4 - 1/2]$. However there can be at most two values of k in this range with $|pk^2 + pk + (p - q)/4| < \sqrt{d}/2$, and so there are at most two primes $Q < \sqrt{d}/2$ with $(Q/d) = 1$. This immediately restricts the number of reduced forms of discriminant d, as for every reduced form (a, b, c) at least one of $|a|$ or $|c|$ is less than $\sqrt{d}/2$. From this we deduce that the length of the principal class is less than or equal to 10 and that the class number is one.

2. Binary quadratic forms: notation and theory.

The proof of Theorem 1 uses the elementary theory of binary quadratic forms, for which we refer the reader to [Bu]. We do however note a few definitions which are used frequently in our proofs:

We denote by (a, b, c) a binary quadratic form of discriminant d. A form (a, b, c) of discriminant $d > 0$ is said to be *reduced* if

$$0 < b < \sqrt{d}, \quad \sqrt{d} - b < 2|a| < \sqrt{d} + b.$$

Note that these conditions imply that $b > 0$ and $ac < 0$. Moreover $b^2 \equiv d \bmod 4|a|$ and $\sqrt{d} - 2|a| < b < \sqrt{d}$, so that if $|a|$ is a given odd prime then there are just two possibilities for b. If $|a| = 1$ then there is a unique possibility for b, the largest integer $< \sqrt{d}$ which is of the same parity as d.

The form (a', b', c') is said to be *right adjacent* to (a, b, c) if $a' = c$ and $b + b' \equiv 0 \bmod 2c$. Also then (a, b, c) is said to be *left adjacent* to (a', b', c'). We write

$$(a, b, c) \sim (a', b', c').$$

The above inequalities imply that there are finitely many reduced binary quadratic forms of discriminant d, and thus they form *cycles*. Since the signs of the a-coefficient in adjacent forms are opposite, any cycle is of even length.

Henceforth we assume the hypothesis of Theorem 1 holds. Evidently b is always odd since $b^2 \equiv d \equiv 1 \bmod 4$. Note that we know that $h(d)$ is odd, since $d = pq$ with $p \equiv q \equiv 3 \bmod 4$ ([C2]).

Now, observe that

$$\left| pk^2 + pk + \frac{p - q}{4} \right| = \left| \frac{(2k+1)^2 p - q}{4} \right|;$$

and when $0 \le k \le \sqrt{d}/4 - 1/2$, we have $1 \le 2k + 1 \le \sqrt{d}/2$. Hence the assumption in Theorem 1 is equivalent to the following:

$f_p(x)$ is prime or equal to 1 for all odd integers x with $1 \le x \le \sqrt{d}/2$, where

$$f_p(x) := \left| \frac{px^2 - q}{4} \right|.$$

We denote by M and m the largest odd integers less than $\sqrt{d}$ and $\sqrt{q/p}$ respectively. Note that, by definition, there is a unique reduced form (a, b, c) with $a = 1$, namely $(1, M, -(d - M^2)/4)$. We also let $p_1 = f_p(m)$ and $p_2 = f_p(m + 2)$.

It should be noted that the class number $h(d)$ here is the number of ordinary equivalence classes associated with 2×2 integer transformation matrices of determinant ± 1 as opposed to the narrow class number which is the number of strict equivalence classes obtained by transformation matrices of determinant 1. For the relation between the two class numbers see Theorem 3, page 198 in [C1]. In the case when $d = pq$ with p and q congruent to 3 mod 4 the forms (a, b, c) and $(-a, b, -c)$ while strictly inequivalent are equivalent in the ordinary sense.

3. Preparatory lemmas. Throughout this section we assume that the hypothesis of Theorem 1 holds and that we are working only with binary quadratic forms of discriminant d. In fact we shall assume $d > 4616$ as we can check computationally up to there.

Lemma 1. *The only reduced form $(a, b', -c)$ with $a, c > 0$ where p divides a is $(p, pm, -p_1)$.*

Proof. As p divides d, the form $(a, b', -c)$ is of the form $(pn, pb, -c)$. By definition of reduced form we have $pb < \sqrt{d}$ or $b < \sqrt{q/p} < \sqrt{d}/2$. Hence by assumption $|(pb^2 - q)/4| = |(p^2b^2 - d)/(4p)| = nc$ is prime or equal to 1. This gives either $n = 1$ and so $a = p$, or $a = pn$ where n is prime and $c = 1$.

If $a = p$ then by definition of reduced form we have $\sqrt{pq} - pb < 2p$ or $\sqrt{q/p} - 2 < b$ and $bp < \sqrt{pq}$, which gives $b < \sqrt{q/p}$. Hence $\sqrt{q/p} - 2 < b < \sqrt{q/p}$ and thus $b = m$.

Next if $a = pn$ we have the reduced form $(pn, pb, -1)$. Consider the form (A, B, pn) left adjacent to $(pn, pb, -1)$. Then pn divides $B + pb$ so that p divides B. We write $B = pk$; since B is odd and $0 < B < \sqrt{d}$, it follows that k is odd and $k < \sqrt{d}/p = \sqrt{q/p}$. Thus $f_p(k) = |(B^2 - d)/(4p)| = |An|$ is prime or equal to 1 by hypothesis, and so $A = \pm 1$ since n is prime; in fact $A = -1$ since $A(pn) < 0$. There is a unique reduced form of discriminant d with first coefficient -1 and so $k = b$; therefore $(-1, pb, pn) \sim (pn, pb, -1)$, so that n divides b (by the definition of adjacency), and thus n divides $(pb)^2 + 4pn = d$, which is untrue.

Lemma 2. *There are no more than two odd positive integers x for which $f_p(x) \le \sqrt{d}/2$. The only possibilities are $x = m$ or $x = m + 2$.*

Proof. We prove that $f_p(x) > \sqrt{d}/2$ for $x < m$ and for $x > \sqrt{q/p} + 1$; the lemma then follows from the definition of m. If $x > \sqrt{q/p} + 1$ then $(px^2 - q)/4 > p/4 + \sqrt{d}/2 > \sqrt{d}/2$. When $x < m$ we need only consider when $m \geq 3$. Then $1 \leq x \leq m-2 < \sqrt{q/p}-2$, so that $(q-px^2)/4 > \sqrt{d}-p$. As $\sqrt{q/p} > m \geq 3$, we have $p < \sqrt{d}/3$, so that $(q-px^2)/4 > \sqrt{d}-p > (2\sqrt{d})/3 > \sqrt{d}/2$.

LEMMA 3. *If Q is prime with $(d/Q) = 1$ and $Q \leq \sqrt{d}/2$, then $Q = f_p(x)$ for some odd positive integer $x \leq \sqrt{d}/2$.*

Proof. We can find a solution px to the congruence $y^2 \equiv d \bmod 2pQ$ with $0 \leq px \leq pQ$ (since p divides d). Since $0 < x \leq Q < \sqrt{d}/2$ is odd, we know that $f_p(x)$ is prime or 1 by assumption. Moreover $f_p(x) = |((px)^2-d)/(4p)|$ is divisible by Q since Q is odd, and thus $f_p(x) = Q$.

LEMMA 4. *If $2f_p(x) < \max\{x-1, \sqrt{d}/2 - x\}$ for some odd positive $x \leq \sqrt{d}/2$, then $f_p(x) = 1$.*

Proof. Write $l = f_p(x) = |(q-px^2)/4|$.

If $2l \leq \sqrt{d}/2 - x$ then $f_p(x+2l) = l(p(x+l) \pm 1)$ and $1 \leq x \leq x+2l \leq \sqrt{d}/2$. By assumption $f_p(x+2l)$ is prime or equal to 1, which gives $l=1$ since $p(x+l) \pm 1 \geq 3(1+0)-1 = 2$.

If $2l \leq x-1$ then $f_p(x-2l) = l(p(x-l) \pm 1)$ and $1 \leq x-2l \leq x$. By assumption $f_p(x-2l)$ is prime or equal to 1, which gives $l=1$ since $p(x-l) \pm 1 \geq 3(l+1)-1 \geq 2$.

LEMMA 5. *There are no primes Q with $Q \leq \sqrt{d}/8 - 1/4$ such that $(d/Q) = 1$.*

Proof. By Lemma 3, if such a Q exists, then $Q = f_p(x)$ for some odd positive integer $x \leq \sqrt{d}/2$. Then $2f_p(x) = 2Q \leq \sqrt{d}/4 - 1/2 \leq \max\{x-1, \sqrt{d}/2 - x\}$, and so $Q = 1$ by Lemma 4, giving a contradiction.

LEMMA 6. *There are no more than two primes $Q \leq \sqrt{d}/2$ for which $(d/Q) = 1$. The only possibilities are $p_1 = f_p(m)$ and $p_2 = f_p(m+2)$.*

Proof. By Lemma 3, $Q = f_p(x)$ for some x. By Lemma 2, $x = m$ or $x = m+2$.

LEMMA 7. *All reduced forms are of the form (a,b,c) where $|a|$ and $|c|$ are each either primes or 1, provided $d \geq 4616$.*

Proof. If p divides a or c then the form is given by Lemma 1; so henceforth assume p does not divide ac. As (a,b,c) is reduced, $|a|, |c| < \sqrt{d} < q$, so q does not divide ac.

Let Q be the smallest prime that divides ac; from the above, Q can be assumed to be neither p nor q. Now $b^2 \equiv d \bmod Q$ so that $(d/Q) = 0$ or 1, and thus $(d/Q) = 1$. If one of $|a|$ or $|c|$ is composite then $Q < d^{1/4} \leq \sqrt{d}/8 - 1/4$, which is impossible, by Lemma 5.

4. The proof of Theorem 1. We first prove that the number of reduced forms is less than or equal to 10.

By Lemma 7 if (a,b,c) is a reduced form, then $|a|$ and $|c|$ are either primes or 1. One of $|a|$ and $|c|$ is less than $\sqrt{d}/2$, and so, by Lemma 6, the only possible values for this number are 1, p, p_1 or p_2. Note that if (a,b,c) is reduced then (c,b,a) is also reduced; also, for every prime Q with $(d/Q)=1$, there are at most two reduced forms (Q,b,c). Since one of our forms is $(p,pm,-p_1)$, we deduce that the total number of reduced forms is less than or equal to 10. (Note here that (a,b,c) and $(-a,b,-c)$ are considered to be identical.)

In Section 2 we noted that the class number is odd and that every equivalence class of forms contains an even number of forms.

Assume that there is an equivalence class of forms with exactly two forms, namely $(a,b,c)\sim(c,b',a)$, since these forms are both left and right adjacent to each other. We note that, to have the same discriminant, and since $b,b'>0$, we must have $b=b'$. Thus both a and c divide b, and so ac divides $b^2-4ac=d$. Since $q>|a|$, $|c|$ we see that $ac=-1$ or $-p$. We cannot have $ac=-1$ since then $d=b^2+4$ so that $(-1/p)=1$, contradicting $p\equiv 3 \bmod 4$. Thus we may assume $a=p$ and $c=-1$, which gives $d=p^2m^2+4p$ by Lemma 1. Thus $p_1=1$ and $p_2>\sqrt{d}/2$ and we have accounted for all of the forms. In other words, d is of the form $d=p^2m^2+4p$, with $h(d)=1$ and the principal cycle is $(1,pm,-p)\sim(-p,pm,1)$.

Otherwise each equivalence class of forms has ≥ 4 forms. Given that there are ≤ 10 reduced forms this means that $h(d)\leq 2$. However $h(d)$ is odd so $h(d)=1$.

Remark. For those d in (ii) one can write down their principal cycles: If $d=p^2s^2+4p$ then $p_1=1,\ p_2>\sqrt{d}/2$ and the principal cycle is

$$(1,ps,-p)\sim(-p,ps,1).$$

If $d=p^2s^2-4p$ then $p_2=1,\ p_1=ps-p-1$ and the principal cycle is

$$\begin{aligned}(1,ps-2,-p_1)&\sim(-p_1,p(s-2),p)\sim(p,p(s-2),-p_1)\\&\sim(-p_1,ps-2,1).\end{aligned}$$

If $d=4p^2s^2-p$ then $p_1=ps-(p+1)/4<\sqrt{d}/2<p_2$ and the principal cycle is

$$\begin{aligned}(1,2ps-1,-p_1)&\sim(-p_1,p(2s-1),p)\sim(p,p(2s-1),-p_1)\\&\sim(-p_1,2ps-1,1).\end{aligned}$$

If we wished to extend our proof above to directly show that (i) implies (ii), then note that the case $p_1=1$ leads to d of the form p^2s^2+4p, and $p_2=1$ leads to d of the form p^2s^2-4p. One might try to extend this case-by-case analysis to complete such a proof.

References

[Bu] D. Buell, *Binary Quadratic Forms*, Springer, New York, 1989.

[C1] H. Cohn, *Advanced Number Theory*, Dover, New York, 1980.

[C2] —, *A Second Course in Number Theory*, Wiley, New York, 1962.

[L1] S. Louboutin, *Prime producing quadratic polynomial and class numbers of real quadratic fields*, Canad. J. Math. 42 (1990), 315–341.

[L2] —, *Addendum to "Prime producing quadratic polynomial and class numbers of real quadratic fields"*, ibid. 42 (1990), 1131.

[Mo] R. A. Mollin, *Quadratics*, CRC Press, Boca Raton, 1996.

[MW] R. A. Mollin and H. C. Williams, *On a determination of real quadratic fields of class number one and related continued fraction period length less than 25*, Proc. Japan Acad. 67 (1991), 20–25.

Department of Mathematics
University of Puerto Rico
Humacao, Puerto Rico 00791
U.S.A.
E-mail: as@cuhwww.upr.clu.edu

Current address:
School of Mathematics, TIFR
Homi Bhabha Road
Colaba
Mumbai 400 005, India
E-mail: anitha@math.tifr.res.in

Received on 3.4.1997
and in revised form on 17.12.1998 (3159)