Canad. Math. Bull. Vol. **32** (4), 1989

QUADRATIC NON-RESIDUES AND PRIME-PRODUCING POLYNOMIALS

BY

R. A. MOLLIN AND H. C. WILLIAMS

ABSTRACT. We will be looking at quadratic polynomials having positive discriminant and having a long string of primes as initial values. We find conditions tantamount to this phenomenon involving another long string of primes for which the discriminant of the polynomial is a quadratic non-residue. Using the generalized Riemann hypothesis (GRH) we are able to determine *all* discriminants satisfying this connection.

1. **Introduction.** There has been a certain fascination throughout mathematical history with prime-producing quadratic polynomials. The most celebrated of these is the one discovered by Euler [1] in 1722, namely; $x^2 - x + 41$ is prime for all integers x with $1 \leqq x \leqq 40$, (or Legendre's version $x^2 + x + 41$ is prime for $0 \leqq x \leqq 39$). The discriminant of the Euler polynomial is -163. This is related to Gauss' class number one problem for complex quadratic fields. For a discussion of the history and solution of this problem there is an excellent article [2] by D. Goldfeld.

It is well-known that:

THEOREM 1.1. *Let $d > 7$ be an integer with $d \equiv 3 \pmod 4$, then the following are equivalent:*
(1) *The polynomial $f_d(x) = x^2 + x + (d+1)/4$ is prime for all integers x with $0 \leqq x \leqq (d-7)/4$.*
(2) $(-d/p) = -1$ *for all odd primes $p < (d+1)/4$ and $d \equiv 3 \pmod 8$ where $(*/*)$ is the Legendre symbol.*

Employing the solution of the class number one problem for complex quadratic fields one gets:

COROLLARY 1.1. *Let $d \equiv 3 \pmod 8$ be a positive square-free integer. Thus, $(-d/p) = -1$ for all primes $p < (d+1)/4$ if and only if $d \in \{3, 11, 19, 43, 67, 163\}$.*

The situation for quadratic polynomials of positive discriminant is not so neat, and in general is substantially more difficult as we will see in the next section.

Received by the editors March 18, 1988 and, in revised form, November 16, 1988.
1980 Mathematical Subject Classification Numbers: Primary 12A20, Secondary 12A25.
The first author's research is supported by NSERC Canada Grant No. A8484.
The second author's research is supported by NSERC Canada Grant No. A7649.
© Canadian Mathematical Society 1988.

https://doi.org/10.4153/CMB-1989-068-1 Published online by Cambridge University Press

2. **Positive discriminants.** Using the techniques of [3]–[7] it can be shown that the following analogue of Theorem 1.1 holds.

THEOREM 2.1. *If $d > 17$ is a positive integer and $d \equiv 1 \pmod 4$ then the following are equivalent:*
(1) *The polynomial $f_d(x) = -x^2 + x + (d-1)/4$ is prime for all integers x with $1 < x < (\sqrt{d-1})/2$.*
(2) *$(d/p) = -1$ for all odd primes $p < (\sqrt{d-1})/2$ and $d \equiv 5 \pmod 8$.*

Similarly the following results for $d \not\equiv 1 \pmod 4$ can be verified using the techniques of [3]–[7].

THEOREM 2.2. *If $d \equiv 2 \pmod 4$ and $d \neq 2p^2$ for any prime p then the following are equivalent:*
(1) *$f_d(x) = -2x^2 + d/2$ is prime or 1 for all integers x with $0 \leqq x \leqq \sqrt{d}/2$*
(2) *$(d/p) = -1$ for all odd primes $p < \sqrt{d/2}$.*

THEOREM 2.3. *Let $d \equiv 3 \pmod 4$ be a positive integer with $d \neq 2p^2 + 1$ for any prime p. Then the following are equivalent:*
(1) *$f_d(x) = -2x^2 + 2x + (d-1)/2$ is prime or 1 for all integers x with $0 < x \leqq (\sqrt{d-1})/2$.*
(2) *$(d/p) = -1$ for all odd primes $p < (\sqrt{d-2})/2$.*

The following tables 2.1 and 2.2 illustrate Theorems 2.2 and 2.3:

TABLE 2.1

d	$f_d(x) = -2x^2 + d/2$ for $0 \leqq x < (\sqrt{d})/2$
6	3, 1
10	5, 3
14	7, 5
26	13, 11, 5
38	19, 17, 11, 1
62	31, 29, 23, 13
122	61, 59, 53, 43, 29, 11
362	181, 179, 173, 163, 149, 131, 109, 83, 53, 19
398	199, 197, 191, 181, 167, 149, 127, 101, 71, 37

Now we use the GRH to show that Tables 2.1 and 2.2 contain *all* the values.

Set $b = b(d) = [\sqrt{d/2}]$ if $d \equiv 2 \pmod 4$ and $b = [(\sqrt{d-1})/2]$ if $d \equiv 3 \pmod 4$. Our problem is to find all $d \equiv 2$ or $3 \pmod 4$ such that:

$$(*) \qquad (d/p) = -1 \text{ for all odd primes } p < b(d).$$

We first set $S(t) = \sum_{p<t}(d/p)$, where the sum is taken over all odd primes $p < t$. In order for $(*)$ to hold up we must have:

$$|S(b)| = \pi(b) - 1 - \epsilon$$

https://doi.org/10.4153/CMB-1989-068-1 Published online by Cambridge University Press

TABLE 2.2

d	$f_d(x) = -2x^2 + 2x + (d-1)/2$ for $0 < x \leqq (\sqrt{d} - 1)/2$
3	—
7	3
11	5
15	7
23	11, 7
35	17, 13
47	23, 19, 11
83	41, 27, 29, 17
143	71, 67, 59, 47, 31
167	83, 79, 71, 59, 43, 23
227	113, 109, 101, 89, 73, 53, 29

where as usual, $\pi(x)$ denotes the number of primes $\leqq x$ and $\epsilon = 0$ unless b is a prime, in which case $\epsilon = 1$.

If we denote by $\Delta(= 4d)$ the discriminant of $Q(\sqrt{d})$, then for $X(p) = (\Delta/p)$ and

$$A(t) = \sum_{p<t} X(p),$$

we get $A(t) = S(t)$. Also, by assuming the truth of the *GRH*, we can use Theorem 3 of Oesterlé [8] (see [5]) to get

$$|A(t)| < B(t, \Delta),$$

where

$$B(t, \Delta) = \sqrt{t}\left(\left\{\frac{1}{\pi} + \frac{5.3}{\log t}\right\}\log \Delta + 2\left\{\frac{\log t}{2\pi} + 2\right\}\right).$$

From a result of Rosser and Schoenfeld [10], we have

$$\pi(t) - 1 - \epsilon > (t/\log t) - 1 - \epsilon = T(t)$$

for $t > 17$. If we put $t = b(d)$, it can be shown that for all $d > 10^{11}$ we have

$$B(b, 4d) < T(b).$$

Hence, if $(*)$ holds and $d > 10^{11}$, we have

$$|S(b)| = |A(b)| < B(b, 4d) < T(b) < |S(b)|,$$

a contradiction. It follows that if condition $(*)$ is satisfied by some d, then $d < 10^{11}$.

We need now deal only with values of $d < 10^{11}$. We denote by $N_i(q)$ the least positive integer N such that $N \equiv i \pmod 4$ and $(N/p) = -1$ for all odd primes

https://doi.org/10.4153/CMB-1989-068-1 Published online by Cambridge University Press

TABLE 2.3

q	$N_2(q)$	$N_3(q)$
3	2	11
5	2	23
7	38	47
11	62	83
13	362	83
17	362	167
19	398	167
23	398	227
29	398	13163
31	398	23327
37	47318	23327
41	64382	69467
43	238262	69467
47	238262	116387
53	238262	331427
59	430022	331427
61	430022	14853467
67	30356618	19739387
71	52642322	59055167
73	52642322	59089103
79	95200838	86374763
83	172712678	86374763
89	231912722	278778407
97	231912722	278778407
101	231912722	361651883
103	231912722	545559467
107	231912722	545559467
109	3668933078	545559467
113	5638787822	2832363203
127	5638787822	2832363203
131	5638787822	7012246247
137	5638787822	7012246247
139	6154772762	7012246247
149	6154772762	7012246247
151	2115451385858	7012246247
157	3356290346702	7012246247
163	—	7012246247
167	—	6821069695523

$p \leqq q$. To compute the values of $N_i(q)$ for various values of q we used a sieving device (UMSU, see Patterson and Williams [9]) at the University of Manitoba. We list in Table 3.3 the results of about a day's run of UMSU.

Consider now the case of $d \equiv 3 \pmod 4$. If $d > 3363$, then $\sqrt{(d-1)}/2 > 29$. The least value of d such that $(*)$ holds for all $p \leqq 29$ is 13163. But if $d \geqq 13163$, then $\sqrt{(d-1)}/2 > 57$; and this means that if (*) is satisfied, then $d \geqq 331427$ and $(\sqrt{d-1})/2 > 287$. Since $N_3(167) > 10^{12}$ then $(*)$ can hold only for values of

https://doi.org/10.4153/CMB-1989-068-1 Published online by Cambridge University Press

$d \leqq 3363$. Similarly, when $d \equiv 2 \pmod 4$, the condition $(*)$ can hold only for values of $d \leqq 2738$.

A direct search of all values of $d \leqq 3363$ revealed that only those values given in Tables 2.1 and 2.2 satisfy condition $(*)$.

We have now proved:

THEOREM 2.4. *Under the GRH, if* $d \equiv 2, 3 \pmod 4$ *and* d *satisfies* $(*)$, *then* d *must be one of the values given in Table* 2.1 *or Table* 2.2.

REFERENCES

1. E. Euler, Mem de Berlin, année 1722, 36; Comm. Arith. **1**, 384.

2. D. Goldfeld, *Gauss' Glass Number Problem for Imaginary Quadratic Fields*, Bull. Amer. Math. Soc. (New Series) **13** (1985), 23–37.

3. R. 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.

4. ———, *Class Number One Criteria for Real Quadratic Fields I*, Proceedings Japan Acad. Ser. A. **63** (1987), 121–125.

5. R. Mollin and H. Williams, *A Conjecture of S. Chowla via the Generalized Riemann Hypothesis*, Proceedings Amer. Math. Soc. **102** (1988), 794–796.

6. ———, *On Prime-Valued Polynomials and Class Numbers of Real Quadratic Fields*, Nagoya Math. J. **112** (1988), 143–151.

7. ———, *Prime Producing Quadratic Polynomials and Real Quadratic Fields of Class Number One* (to appear: Proceedings of the International Number Theory Conference at Quebec City, July 1987).

8. Oesterlé, *Versions effectives du théorèm de Chebotarev sous L'Hypothèse de Riemann Gènèralisé*, Soc. Math. France Astérisque **61** (1979), 165–167.

9. C. D. Patterson and H. C. Williams, *A report on the University of Manitoba Sieve Unit*, Congresses Numerantium **37** (1983), 85–98.

10. J. B. Rosser and L. Schoenfeld, *Approximate Formulas for Some Functions of Prime Numbers*, Illinois J. Math. **6** (1962), 64–94.

Mathematics Dept.,
University of Calgary,
Calgary, Alberta,
T2N 1N4,
Canada

Computer Science Dept.,
University of Manitoba,
Winnipeg, Manitoba,
R3T 2N2,
Canada

https://doi.org/10.4153/CMB-1989-068-1 Published online by Cambridge University Press