PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 43, Number 2, April 1974

PRIME QUADRATICS ASSOCIATED WITH COMPLEX QUADRATIC FIELDS OF CLASS NUMBER TWO

M. D. HENDY

ABSTRACT. We establish a necessary and sufficient relation between those quadratic fields of class number two, and some quadratic polynomials $f(x)$ which take only prime values for small positive integers.

Euler discovered that for certain primes q, namely $q=2, 3, 5, 11, 17, 41$, the quadratic

$$f(x) = x^2 + x + q \tag{1}$$

takes only prime values for integers in the interval $0 \leqq x \leqq q-2$. (Cf. [1].) In fact it is known that a prime q is such a value if and only if the complex quadratic field $Q(\sqrt{(1-4q)})$ has class number one. This test readily gives rise to all the fields $Q(\sqrt{-d})$ with $d \geqq 7$, which have class number one. In a similar manner we discover a quadratic similar to (1) related to each of the complex quadratic fields of class number two.

Let d be any squarefree positive integer, and h be the class number of the field $Q(\sqrt{-d})$. This field has discriminant $D=-d$ when $d \equiv 3 \pmod 4$, or $D=-4d$ otherwise. From the theory of genera of complex quadratic fields, we note that the class group of $Q(\sqrt{-d})$ will contain one factor of order a power of two if and only if D has precisely two distinct prime factors. Hence h can only be two for fields $Q(\sqrt{-d})$ of one of the following three types:

I. $d=2p$, p odd prime, $D=-8p$.

II. $d=p \equiv 1 \pmod 4$, p prime, $D=-4p$.

III. $d=pq \equiv 3 \pmod 4$, p, q prime, $D=-pq$.

For fields of Type III, we will assume that $p<q$. For each field we associate a quadratic $f(x)$ similar to (1). For fields of Type I,

$$f(x) = 2x^2 + p. \tag{2}$$

Received by the editors June 7, 1971 and, in revised form, February 14, 1972 and July 30, 1973.

AMS (MOS) subject classifications (1970). Primary 12A25, 12A50; Secondary 10H15.

Key words and phrases. Complex quadratic fields, class number, prime integers, ideals, principal ideals.

For fields of Type II,

$$f(x) = 2x^2 + 2x + (p + 1)/2. \tag{3}$$

For fields of Type III,

$$f(x) = px^2 + px + (p + q)/4. \tag{4}$$

THEOREM. *A complex qua ratic field of Type* I, II *or* III *has class number* $h=2$ *if and only if the corresponding quadratic* $f(x)$ *takes only prime values for integers* x *in the interval* $0 \leqq x < k$, *where* $k=\sqrt{(p/2)}$ *for fields of Type* I, $k=(\sqrt{p}-1)/2$ *for fields of Type* II, *and* $k=\sqrt{(pq/12)}-\frac{1}{2}$ *for fields of Type* III.

PROOF. The proof is established via the following lemmas.

LEMMA 1. *If* x *is the least positive integer for which* $f(x)=2x^2+p$ *of* (2) *is composite, then* $x<(p-1)/\sqrt{2} \Rightarrow x<\sqrt{(p/2)}$.

PROOF. $f(p)$ is composite, so a minimal positive integer x for which $f(x)$ is composite does exist. Set $L_0=(p-1)/\sqrt{2}$, $L=\sqrt{(p/2)}$ and $L_n=\sqrt{(L_0^2 2^{-n}+(2^n-1)p2^{-n-1})}$, and suppose $x<L_0$. We find, for $n \geqq 0$,

$$L < L_{n+1} < L_n \leqq L_0, \tag{5}$$

$$L = \lim_{n \to \infty} L_n \quad \text{and} \tag{6}$$

$$L_{n+1} = \tfrac{1}{2}\sqrt{(2L_n^2 + p)}. \tag{7}$$

Suppose, for some $n \geqq 0$, $x<L_n$. As $f(x)$ is composite let a be its least prime divisor. Thus

$$a^2 \leqq f(x) < 2L_n^2 + p \leqq 2L_0^2 + p = (p-1)^2 + p < p^2, \tag{8}$$

and, in particular,

$$a < \sqrt{(2L_n^2 + p)} < p. \tag{9}$$

Thus $f(y)=a$ has no real roots. Now

$$f(|x - a|) \equiv f(x) \equiv 0 \pmod{a}, \tag{10}$$

so that $f(|x-a|)$ also has a as a proper divisor, and hence is composite. $f(0)=p$, so $x \neq a$, and as x is minimal $x<|x-a|$, i.e.,

$$x \leqq a/2 < \tfrac{1}{2}\sqrt{(L_n^2 + p)} = L_{n+1}. \tag{11}$$

Thus by induction $x<L_0 \Rightarrow x<L_n$ for each $n \geqq 0$, and so $x \leqq \lim_{n\to\infty} L_n = L$. Equality cannot hold as L is irrational, so $x<L$ establishing the lemma.

LEMMA 2. *If x is the least positive integer for which $f(x)=2x^2+2x+(p+1)/2$ of (3) is composite, then $x<(p-\sqrt{2})/2\sqrt{2}\Rightarrow x<(\sqrt{p}-1)/2$.*

PROOF. We use the same procedure as above in Lemma 1, with $L=(\sqrt{p}-1)/2$, $L_0=(p-\sqrt{2})/2\sqrt{2}$ and

$$L_n = \sqrt{((L_0 + \tfrac{1}{2})^2 2^{-n} + (2^n-1)p2^{-n-2})} - \tfrac{1}{2}.$$

In equation (10) we replace $f(x-a)\equiv f(a-x)\equiv f(x)\equiv 0 \pmod a$ with $f(x-a)\equiv f(a-x-1)\equiv f(x)\equiv 0 \pmod a$, so for x minimal, $x<a$ and $x<a-x-1$. The remainder of the proof then follows.

Unfortunately a corresponding result for $f(x)=px^2+px+(p+q)/4$ of (4) does not exist for $p>3$. For fields of Types I and II set $a=2$ and for fields of Type III set $a=p$. Let A be the ambiguous ideal with $N(A)=a$. This meaning of the letter a has nothing to do with its use in Lemmas 1 and 2. From now on a will have the meaning specified here.

LEMMA 3. *If $h>2$, then there exist nonprincipal ideals B, C with the following properties*:

1. *B and C are neither principal nor in the same class as A.*
2. *ABC is principal.*
3. *B is a prime ideal.*
4. *$1<N(B)$, $N(C)<\sqrt{(-D/3)}$.*
5. *$A\nmid BC$.*

PROOF. As $N(A)<-D/4$, A cannot be principal. Let K_1 be the class of principal ideals and K_2 the class containing A. As $h>2$ and $K_2^2=K_1$, $\{K_1, K_2\}$ is a proper subgroup of the class group. Hence there exist other classes, and at least one of them, say K_3, has a prime ideal B as its member of least norm. As K_3 is distinct from K_1, K_2, so too is $K_4=K_2K_3^{-1}$. Let C be an ideal of least norm of K_4, so that $ABC\in K_2K_3K_4=K_2^2=K_1$ is a principal ideal.

We have an upper bound (see [1, p. 141]) on the size of the least (according to norm) ideal of any equivalence class K_i. That is, in each class K_i over $Q(\sqrt{-d})$ there exists an ideal A_i, with $N(A_i)<\sqrt{(-D/3)}$. Hence B, C are ideals satisfying properties 1, 2, 3 and 4.

Further $A\mid BC\Rightarrow A\mid C$ as B is prime, so that there would need to exist an ideal E, with $C=AE$. This would mean $BE\sim A^2BE=ABC$, so BE is principal; however, as $N(E)\leqq N(C)/2<\frac{1}{2}\sqrt{(-D/3)}$, $N(B)<\sqrt{(-D/3)}$, and $N(BE)<-D/6$ it could not be principal. Hence $A\nmid BC$.

LEMMA 4. *In the fields of Type* I, *$h>2\Rightarrow f(x)$ is composite for some integer x in the interval $0\leqq x<\sqrt{(p/2)}$.*

PROOF. $N(A)=2$. From Lemma 3, there exist ideals B, C with properties 1 to 5. Set $b=N(B)$, $c=N(C)$. As ABC is principal there exist

integers y, z satisfying

$$N(ABC) = 2bc = y^2 + 2pz^2. \tag{12}$$

Thus $2|y$. Let $y=2x$, so that (12) gives

$$bc = 2x^2 + pz^2. \tag{13}$$

$A\nmid BC$, so $2\nmid bc$ and z is odd. Further

$$bc = N(BC) < -D/3 = 8p/3 < 4p, \tag{14}$$

so, from (14), $z^2=1$, and (13) becomes

$$bc = 2x^2 + p = f(x). \tag{15}$$

From (15), $x^2=(bc-p)/2<5p/6$, so, for $p>3$, $x<\sqrt{(5p/6)}<(p-1)/\sqrt{2}$. Further for $p=3$, as x is integral $x<\sqrt{(5/2)}\Rightarrow x\leqq 1<\sqrt{2}=(p-1)/\sqrt{2}$. Hence

$$x < (p-1)/\sqrt{2}, \tag{16}$$

so, by Lemma 1, $f(x)$ is composite for some integer x in the interval $0\leqq x<\sqrt{(p/2)}$.

LEMMA 5. *In fields of Type* II, $h>2\Rightarrow f(x)$ *is composite for some integer* x *in the interval* $0\leqq x<(\sqrt{p}-1)/2$.

PROOF. As above we can find $b=N(B)$, $c=N(C)$ and integers y, z so that

$$N(ABC) = 2bc = y^2 + pz^2. \tag{17}$$

From Lemma 3, $2\nmid bc$, so

$$2bc \equiv 2 \equiv y^2 + z^2 \pmod 4, \tag{18}$$

and hence both y and z are odd. Putting $y=2x+1$ we obtain

$$bc = 2x^2 + 2x + (1 + pz^2)/2, \tag{19}$$

and further

$$bc = N(BC) < -D/3 = 4p/3 < 2p. \tag{20}$$

Thus $z^2=1$, and (19) becomes

$$bc = 2x^2 + 2x + (p+1)/2 = f(x). \tag{21}$$

Also, from (20), $2x^2+2x+(p+1)/2<4p/3$, so $(x+\frac{1}{2})^2<5p/12\leqq p^2/12\leqq p^2/8$ (as $p\geqq 5$). Hence

$$0 \leqq x < (p-\sqrt{2})/2\sqrt{2}. \tag{22}$$

However, from Lemma 2, $f(x)$ is composite for some integer x in the interval $0 \leqq x < (\sqrt{p}-1)/2$.

LEMMA 6. *In the fields of Type* III, $h>2 \Rightarrow f(x)$ *is composite for some integer* x *in the interval* $0 \leqq x < \sqrt{(-D/12)} - \frac{1}{2}$.

PROOF. We may assume $pq>16$, since $Q(\sqrt{-pq})$ has class number greater than two. $N(A)=p$. As above we can find $b=N(B)$, $c=N(C)$ and integers y, z, $y \equiv z \pmod 2$ so that

$$N(ABC) = pbc = (y^2 + pqz^2)/4, \tag{23}$$

i.e.,

$$4pbc = y^2 + pqz^2. \tag{24}$$

If $b=2$, then $(2|pq)=1$, so $pq \equiv 7 \pmod 8$, and hence $p+q \equiv 0 \pmod 8$. Thus, since $pq>16$, we find that $f(0)=(p+q)/4$ is properly divisible by 2 and hence composite.

For $b>2$, from (24), $p|y$, so let $y=pv$, so that (24) becomes

$$4bc = pv^2 + qz^2. \tag{25}$$

As $A \nmid BC$, $p \nmid bc$, and hence $z \neq 0$. Also if $v=0$, then $q|bc$. However b, $c < \sqrt{(pq/3)} < q$ so $q \nmid b$, c and as q is prime $q \nmid bc$. Hence $v \neq 0$. b, p are primes, $(b, p)=1$, so $b|z \Rightarrow b|v$, so, from (25),

$$\begin{aligned} b \mid z &\Rightarrow 4c > (p+q)b > 2(p+q) \\ &\Rightarrow 4c^2 > p^2 + q^2 + 2pq > 2pq \\ &\Rightarrow c > \sqrt{(pq/2)}. \end{aligned}$$

However as $c < \sqrt{(pq/3)}$, $b \nmid z$. Thus $z \not\equiv 0 \pmod b$, so there exists an inverse z' of $z \pmod b$. From (25) we obtain

$$p(vz')^2 + q \equiv 0 \pmod b. \tag{26}$$

Let w be the least positive residue $(\bmod b)$ of vz'. As b is odd, one of w, $b-w$ is odd, so let u be that value and hence $0<u<b$. From (26), $pu^2+q \equiv 0 \pmod b$ while also $pu^2+q \equiv p+q \equiv 0 \pmod 4$, so

$$pu^2 + q \equiv 0 \pmod{4b}. \tag{27}$$

Since ABC is principal, and C not principal, neither is AB. Thus $pu^2+q \neq 4b$, for otherwise $4bp=(pu)^2+pq$, and $AB=((pu \pm \sqrt{-pq})/2)$. Thus b is a nontrivial divisor of $(pu^2+q)/4$. As u is odd, let $u=2x+1$ so that

$$(pu^2 + q)/4 = f(x) \tag{28}$$

which has a proper prime divisor b, so is composite. Now

$$0 < x = (u-1)/2 < b/2 - \tfrac{1}{2} < \sqrt{(pq/12)} - \tfrac{1}{2}; \tag{29}$$

so again the lemma holds true.

This now establishes the first half of the theorem. The remainder is established in a final lemma.

LEMMA 7. *For each field of Type* I, II *or* III, *if* $f(x)$ *is composite for some integer* x *in the interval* $0 \leqq x < k$, *then* $h > 2$.

PROOF. Suppose $f(x)$ is composite with $0 \leqq x < k$, so that $f(x) = bc$, with $b, c > 1$, integral and b prime. Now with a as chosen before Lemma 3,

$$\begin{aligned} f(x) = bc \Rightarrow abc &= (2x)^2 + d && \text{for fields of Type I,} \\ &= (2x+1)^2 + d && \text{for fields of Type II,} \\ &= ((2x+1)^2 p^2 + d)/4 && \text{for fields of Type III.} \end{aligned} \tag{30}$$

For fields of Type I, $x \neq 0$, as $f(0) = p$ is prime, so we find that for all fields $(bc, d) = 1$. Hence, from (30), $(-d|r) = 1$ for all primes r dividing bc.

Let α be the algebraic integer $2x + \sqrt{(-d)}$, $(2x+1) + \sqrt{(-d)}$, or $((2x+1)p + \sqrt{(-d)})/2$ in the fields of Types I, II and III respectively. Hence, in all fields of Type I, $x < \sqrt{(p/2)} \Rightarrow N(\alpha) = (2x)^2 + 2p < 4p$, i.e.,

$$N(\alpha) < 2d. \tag{31}$$

Similarly, in fields of Type II, $x < (\sqrt{p} - 1)/2 \Rightarrow N(\alpha) = (2x+1)^2 + p < 2p = 2d$, i.e.,

$$N(\alpha) < 2d. \tag{32}$$

For fields of Type III, $x < \sqrt{(pq/12)} - \tfrac{1}{2} \Rightarrow ((2x+1)^2 p^2 + pq)/4 < p^3 q/12 + pq/4 < p^2 q^2 (1/12 + 1/60)$, i.e.,

$$N(\alpha) < d^2/10. \tag{33}$$

Using these three inequalities we now prove that the algebraic integer α has no nontrivial factorisation. As the coefficient of $\sqrt{(-d)}$ in α is 1, α cannot be divisible by any nontrivial rational integer. Suppose α does have a nontrivial factorisation in algebraic integers,

$$\alpha = \beta\gamma \tag{34}$$

where for $D \equiv 0 \pmod 4$, $\beta = b_1 + b_2\sqrt{(-d)}$, $\gamma = c_1 + c_2\sqrt{(-d)}$, and for $D \equiv 1 \pmod 4$, $\beta = (b_1 + b_2\sqrt{(-d)})/2$, $\gamma = (c_1 + c_2\sqrt{(-d)})/2$, with $b_1 \equiv b_2 \pmod 2$, $c_1 \equiv c_2 \pmod 2$.

If $b_2 = 0$, β would be a rational integer, hence $\beta = \pm 1$. Similarly $c_2 = 0 \Rightarrow \gamma = \pm 1$. Hence for a nontrivial factorisation (34) we require

$b_2, c_2 \neq 0$. For $D \equiv 0 \pmod 4$, $N(\alpha)=N(\beta)N(\gamma)=(b_1^2+db_2^2)(c_1^2+dc_2^2) \geqq d^2$, which contradicts equations (31) and (32). For $D \equiv 1 \pmod 4$,

$$\begin{aligned} N(\alpha) &= (b_1^2 + db_2^2) \cdot (c_1^2 + dc_2^2)/16 \\ &= (b_1^2c_1^2 + d(b_1^2c_2^2 + b_2^2c_1^2) + d^2b_2^2c_2^2)/16. \end{aligned}$$

However as $N(\alpha) < d^2/10$ by equation (33), we must have $b_2^2c_2^2=1$, $b_1^2c_1^2 < d^2$.

Thus, for fields of Types I or II, α can have no nontrivial factorisation (34), and, for fields of Type III, it can only be of the form

$$\begin{aligned} \alpha &= ((2x + 1)p + \sqrt{(-d)})/2 \\ &= ((b_1 + b_2\sqrt{(-d)})/2) \cdot ((c_1 + c_2\sqrt{(-d)})/2), \end{aligned} \tag{35}$$

with $b_2c_2 = \pm 1$, and $|b_1c_1| < d = pq$. By equating real and imaginary parts in equation (35) we find

$$2(2x + 1)p = b_1c_1 - b_2c_2d = b_1c_1 - b_2c_2pq, \tag{36}$$

and

$$2 = b_1c_2 + b_2c_1. \tag{37}$$

As $2(2x+1)p > 0$, $|b_1c_1| < pq$, and $|b_2c_2| = 1$, then $b_2c_2 = -1$ for (36) to hold. Suppose $b_2 = 1$, $c_2 = -1$; then, by equation (37), $c_1 = b_1 + 2$, and equation (36) becomes

$$2(2x + 1)p = b_1(b_1 + 2) + pq. \tag{38}$$

Hence $p | b_1$ or $p | b_1 + 2$, so $p \leqq \min(|b_1|, |b_1+2|)$. $b_1 \neq -1$, so $b_1(b_1+2) \geqq 0$, and $p(p-2) \leqq b_1(b_1+2)$. Thus it follows from equation (38) that

$$4x + 2 \geqq p + q - 2 \tag{39}$$

and, on squaring,

$$4(2x + 1)^2 \geqq p^2 + q^2 + 2pq - 4p - 4q + 4. \tag{40}$$

However as $p \geqq 3$, $q \geqq 5$, $p^2+q^2 > 4p+4q-4$, so

$$4(2x + 1)^2 > 2pq. \tag{41}$$

Also $x < \sqrt{(pq/12)} - \frac{1}{2}$ so $4(2x+1)^2 < 4pq/3$. This contradicts equation (41), so we cannot have a factorisation with $b_2 = 1$, $c_2 = -1$. Alternatively $b_2 = -1$, $c_2 = 1$ leads to the same contradiction, so the factorisation (34) cannot exist in this case.

Thus in all cases α has no nontrivial factors.

Let A be the ambiguous ideal above. As $(-d|r) = 1$ for all prime divisors of bc, there exist ideals B, C with $N(B) = b$, $N(C) = c$, such that $ABC = (\alpha)$.

Now α has no nontrivial divisors, so ABC has no principal ideal divisors, and in particular none of A, B and AB can be principal. Thus as A^2 is principal, A cannot be in the same class as B, so the number of classes $h>2$.

REFERENCE

1. H. Cohn, *A second course in number theory*, Wiley, New York, 1962. MR **24** #A3115.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF NEW ENGLAND, NEW SOUTH WALES, AUSTRALIA

DEPARTMENT OF MATHEMATICS, MASSEY UNIVERSITY, PALMERSTON NORTH, NEW ZEALAND