REPRESENTATION OF PRIMES BY BINARY QUADRATIC FORMS OF DISCRIMINANT $-256q$ AND $-128q$

by FRANZ HALTER-KOCH

(Received 29 January, 1992)

Introduction. Recently, P. Kaplan and K. S. Williams **[10]** considered (as an example) the representation of primes by binary quadratic forms of discriminant -768. These forms fall into 4 genera, each consisting of two classes. In particular, they considered the forms

$$F = 3X^2 + 64Y^2 \quad \text{and} \quad G = 12X^2 + 12XY + 19Y^2.$$

It follows from genus theory (as explained in **[10]**) that every prime $p \equiv 19 \bmod 24$ is represented by exactly one of the forms F and G. Based on numerical data, they conjectured that a prime $p \equiv 19 \bmod 24$ is represented by

$$\begin{cases} F, & \text{if} \quad V_{(p+1)/4} \equiv 2 \bmod p, \\ G, & \text{if} \quad V_{(p+1)/4} \equiv -2 \bmod p, \end{cases}$$

where

$$V_0 = 2, \qquad V_1 = -4, \qquad V_{n+2} = -4V_{n+1} - V_n \quad (n \geq 0).$$

In this note, we prove this criterion as a special case of a more general result using class field theory and the methods developed in **[4]**.

1. Notations and preliminaries. We start by recalling some facts from Gauss' theory of binary quadratic forms and its relations with class field theory, cf. **[1]** and **[2]**, part III.

Let D be a discriminant of positive definite primitive integral binary quadratic forms (i.e., $D \in \mathbb{Z}$, $D < 0$, $D \equiv 0$ or $1 \bmod 4$), and let $\mathscr{H}(D)$ be the class group of such forms of discriminant D (with respect to proper equivalence) under Gauss' composition. The principal class of $\mathscr{H}(D)$ will always be denoted by I, and we use the notation

$$[a, b, c] = aX^2 + bXY + cY^2 \in \mathbb{Z}[X, Y].$$

We say that a class $C \in \mathscr{H}(D)$ represents an integer w and write $C \to w$, if $w = f(x, y)$ for some form $f \in C$ and $x, y \in \mathbb{Z}$ such that $\gcd(x, y) = 1$. There is a canonical epimorphism

$$\phi_D : \mathscr{H}(4D) \to \mathscr{H}(D)$$

induced by $[a, 2b, 4c] \mapsto [a, b, c]$. If $\bar{C} \in \mathscr{H}(4D)$ and $w \in \mathbb{Z}$ is odd, then obviously $\bar{C} \to w$ implies $\phi_D(\bar{C}) \to w$.

Every discriminant is of the form $D = D_0 f_D^2$, where D_0 is the fundamental discriminant and f_D is the conductor associated with D. The group $\mathscr{H}(D)$ is isomorphic to the ring class group modulo f_D in $\mathbb{Q}(\sqrt{D_0})$. If τ denotes the complex conjugation, then τ acts on the ring class group modulo f_D and hence on $\mathscr{H}(D)$ by $A^\tau = A^{-1}$.

Associated with $\mathscr{H}(D)$, there is a ring class field $k(D)$ over $\mathbb{Q}(\sqrt{D_0})$ and an Artin isomorphism

$$((\cdot)) : \begin{cases} \mathscr{H}(D) \xrightarrow{\sim} \mathrm{Gal}(k(D)/\mathbb{Q}(\sqrt{D_0})) \\ A \mapsto ((A)) \end{cases}$$

https://doi.org/10.1017/S0017089500009824 Published online by Cambridge University Press

possessing the following two fundamental properties;

1) $\mathrm{Gal}(k(D)/\mathbb{Q})$ is given by the splitting group extension

$$1 \to \mathcal{H}(D) \xrightarrow{((\cdot))} \mathrm{Gal}(k(D)/\mathbb{Q}) \to \langle \tau \rangle \to 1;$$

2) For a class $C \in \mathcal{H}(D)$ and a rational prime $p \nmid D$ we have $C \to p$ if and only if $((C)) \in \mathrm{Gal}(k(D)/\mathbb{Q})$ is the Frobenius automorphism of some prime divisor $\mathfrak{P}$ of p in $k(D)$.

We may assume that the Artin isomorphism is normalized in such a way that

$$((\bar{C})) \mid k(D) = ((\phi_D(\bar{C})))$$

for every class $\bar{C} \in \mathcal{H}(4D)$ (observe that, by definition, $((\bar{C})) \in \mathrm{Gal}(k(4D)/\mathbb{Q})$ and $k(4D) \supset k(D)$).

In this note, we shall mainly be concerned with the 2-parts of class groups. We consider the decomposition

$$\mathcal{H}(D) = \mathcal{H}_2(D) \times \mathcal{H}'(D),$$

where $\mathcal{H}_2(D)$ is the 2-Sylow subgroup of $\mathcal{H}(D)$, and $\mathcal{H}'(D)$ is of odd order. We set $h(D) = \#\mathcal{H}(D)$, $h'(D) = \#\mathcal{H}'(D)$, and we denote by $k_2(D) \subset k(D)$ the fixed field of $\mathcal{H}'(D)$ (whence $k_2(D)$ is the maximal 2-extension of $\mathbb{Q}$ inside $k(D)$). For a class $A \in \mathcal{H}_2(D)$, we set

$$[A] = ((A)) \mid k_2(D) \in \mathrm{Gal}(k_2(D)/\mathbb{Q}(\sqrt{D_0})).$$

The following lemma collates the basic properties of the symbol $[\cdot]$.

LEMMA 1. i) *$[\cdot]: \mathcal{H}_2(D) \xrightarrow{\sim} \mathrm{Gal}(k_2(D)/\mathbb{Q}(\sqrt{D_0}))$ is a group isomorphism, and $\mathrm{Gal}(k_2(D)/\mathbb{Q})$ is given by the splitting group extension*

$$1 \to \mathcal{H}_2(D) \xrightarrow{[\cdot]} \mathrm{Gal}(k_2(D)/\mathbb{Q}) \to \langle \tau \rangle \to 1.$$

ii) *Let $C \in \mathcal{H}_2(D)$ be a class satisfying $C^4 = I$, and let p be a rational prime not dividing D. Then we have $C \to p^{h'(D)}$ if and only if the fixed field of $[C]$ in $k_2(D)$ is the decomposition field of p in $k_2(D)$.*

iii) *If $\bar{C} \in \mathcal{H}_2(4D)$, then $\phi_D(\bar{C}) \in \mathcal{H}_2(D)$ and $[\bar{C}] \mid k_2(D) = [\phi_D(\bar{C})]$.*

Proof. i) The canonical epimorphism $\mathcal{H}(D) \to \mathrm{Gal}(k_2(D)/\mathbb{Q}(\sqrt{D_0})$, given by $C \mapsto ((C)) \mid k_2(D)$, has kernel $\mathcal{H}'(D)$; now the assertion follows from the decomposition $\mathcal{H}(D) = \mathcal{H}_2(D) \times \mathcal{H}'(D)$.

ii) It suffices to consider primes p splitting in $\mathbb{Q}(\sqrt{D_0})$; let $\mathfrak{p}$ be a prime divisor of p in $\mathbb{Q}(\sqrt{D_0})$ and $\psi \in \mathrm{Gal}(k(D)/k)$ the Frobenius automorphism of $\mathfrak{p}$. Then $C \to p^{h'(D)}$ is equivalent to $\psi^{h'(D)} = ((C))^{\pm 1}$; since both automorphisms, $\psi^{h'(D)}$ and $((C))^{\pm 1}$, are of 2-power order, we have $\psi^{h'(D)} = ((C))^{\pm 1}$ if and only if $(\psi \mid k_2(D))^{h'(D)} = [C]^{\pm 1}$. Since $C^4 = I$, the last equality holds if and only if $\psi \mid k_2(D)$ and $[C]$ generate the same cyclic subgroup of $\mathrm{Gal}(k_2(D)/\mathbb{Q}(\sqrt{D_0}))$. Since the fixed field of $\psi \mid k_2(D)$ in $k_2(D)$ is exactly the decomposition field of p, the assertion follows.

iii) $[\bar{C}] \mid k_2(D) = \{((\bar{C})) \mid k(D)\} \mid k_2(D) = ((\phi_D(\bar{C}))) \mid k_2(D) = [\phi_D(\bar{C})]$.

https://doi.org/10.1017/S0017089500009824 Published online by Cambridge University Press

2. Class groups of discriminant $-2^t q$. From now on, we consider discriminants of the following two types:

(I) $D = -256q$, q is a prime, $q \equiv 3 \bmod 4$;

(II) $D = -128q$, q is a prime, $q \equiv 3 \bmod 8$

(for these discriminants, $\mathcal{H}_2(D)$ has the same structure as for $D = -768$).
The associated fundamental discriminant is given by

$$D_0 = \begin{cases} -q & \text{in case (I)}, \\ -8q & \text{in case (II)}, \end{cases}$$

and we set, for $s \geq 0$,

$$D_s = 2^{2s} D_0,$$

which implies

$$D = \begin{cases} D_4 & \text{in case (I)}, \\ D_2 & \text{in case (II)}. \end{cases}$$

The group $\mathcal{H}(D_s)$ is isomorphic to the ring class group modulo 2^s in $\mathbb{Q}(\sqrt{D_0})$, and therefore there is an exact sequence

$$(*) \qquad 1 \to \mathcal{P}_0(s) \to \mathcal{H}(D_s) \xrightarrow{\psi_s} \mathcal{H}(D_0) \to 1,$$

where $\psi_s = \phi_{D_{s-1}} \circ \phi_{D_{s-2}} \circ \ldots \circ \phi_{D_0}$, and $\mathcal{P}_0(s)$ is defined as follows: let $\mathcal{P}(s)$ be the prime residue class group modulo 2^s in $\mathbb{Q}(\sqrt{D_0})$, $\mathcal{P}_*(s)$ the subgroup of all $(a \bmod 2^s) \in \mathcal{P}_0(s)$, where either $a \in \mathbb{Z}$ or a is a root of unity, and set $\mathcal{P}_0(s) = \mathcal{P}(s)/\mathcal{P}_*(s)$. By [**5**], $\mathcal{P}_0(s)$ is (for $s \geq 2$) of type

$$\begin{aligned} (2^{s-2}, 2), &\quad \text{if} \quad D_0 \equiv 1 \bmod 8 \text{ or } D_0 = -3, \\ (2^{s-2}, 2, 3), &\quad \text{if} \quad D_0 \equiv 5 \bmod 8, \quad D_0 \neq -3, \\ (2^s), &\quad \text{if} \quad D_0 \equiv 0 \bmod 8. \end{aligned}$$

In case (I), $\mathcal{H}_2(D_0)$ is trivial, and therefore $\mathcal{H}_2(D_s)$ is of type $(2^{s-2}, 2)$ (for $s \geq 2$). In case (II), $\mathcal{H}_2(D_0)$ is of order 2; for $s \geq 1$, $\mathcal{H}_2(D_s)$ is not cyclic by genus theory, and therefore $(*)$ splits. Hence $\mathcal{H}_2(D_s)$ is of type $(2^s, 2)$ in case (II).

In both cases, $\mathcal{H}_2(D)$ is of type $(4, 2)$ and $\mathcal{H}_2(4D)$ is of type $(8, 2)$. We choose generators such that

$$\mathcal{H}_2(4D) = \langle \bar{A}, \bar{B} \rangle, \qquad \bar{A}^8 = \bar{B}^2 = I,$$

and we set

$$A = \phi_D(\bar{A}), \qquad B = \phi_D(\bar{B});$$

then we have

$$\mathcal{H}_2(D) = \langle A, B \rangle, \qquad A^4 = B^2 = I.$$

By means of this normalization it is possible to identify the four ambigous classes of $\mathcal{H}_2(D)$: A^2 and I belong to the principal genus, A^2B and B not; B is the ϕ_D-image of an ambigous form of $\mathcal{H}_2(4D)$, A^2B not.

For these reasons, the four ambiguous classes

$$I, A^2, B, A^2B$$

of $\mathscr{H}^2(D)$ contain the forms

$$\begin{cases} [1,0,64q], [4,4,1+16q], [q,0,64], [4q,4q,q+16] & \text{in case (I)}, \\ [1,0,32q], [4,4,1+8q], [q,0,32], [4q,4q,q+8] & \text{in case (II)}, \end{cases}$$

respectively.

The classes of $\mathscr{H}_2(D)$ fall into 4 genera:

$\mathscr{G}_1 = \{I, A^2\}$, represents numbers $a \equiv 1 \bmod 8$,

$\mathscr{G}_2 = \{B, A^2B\}$, represents numbers $a \equiv q \bmod 8$,

$\mathscr{G}_3 = \{A, A^3\}$ and $\mathscr{G}_4 = \{AB, A^3B\}$.

Let $\alpha, \beta \in \mathbb{Z}$ be such that $(\mathbb{Z}/8\mathbb{Z})^\times = \{\bar{1}, \bar{q}, \bar{\alpha}, \bar{\beta}\}$. Since we are free to replace A by AB, we can normalize the generators in such a way, that $\mathscr{G}_3$ represents numbers $a \equiv \alpha \bmod 8$ and $\mathscr{G}_4$ represents numbers $a \equiv \beta \bmod 8$.

From Lemma 1 and the given description of genera we obtain the following criterion (cf. the Example in [**10**]).

LEMMA 2. *Let D be a discriminant of type* (I) *or* (II) *and p a rational prime satisfying* $\left(\frac{D_0}{p}\right) = 1$. *Then $p^{h'(D)}$ is represented by*

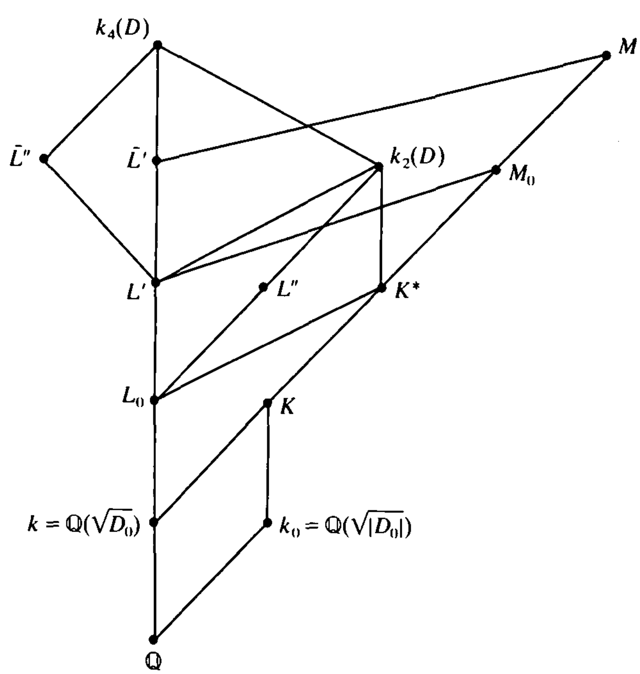
both A and A^3, if $p \equiv \alpha \bmod 8$;

both AB and A^3B, if $p \equiv \beta \bmod 8$;

exactly one of I and A^2, if $p \equiv 1 \bmod 8$;

exactly one of B and A^2B, if $p \equiv q \bmod 8$.

In [**9**] (Corollary on p. 17), we proved a criterion for a prime $p \equiv 1 \bmod 8$ to be represented either by I or by A^2. In the sequel we concentrate our attention to primes $p \equiv q \bmod 8$, and we start by describing the Galois theory of the field $k_2(4D)$ for discriminants D as in (I) or (II).



By Lemma 1, we obtain

$$\mathrm{Gal}(k_2(4D)/\mathbb{Q}) = \langle [\bar{A}], [\bar{B}], \tau \rangle,$$

and $[\bar{A}]^8 = [\bar{B}]^2 = \tau^2 = \mathrm{id}$, $[\bar{A}][\bar{B}] = [\bar{B}][\bar{A}]$, $[\bar{B}]\tau = \tau[\bar{B}]$, $[\bar{A}]\tau = \tau[\bar{A}]^{-1}$.

$k_2(4D)$ possesses 3 subfields on degree 16 containing $k = \mathbb{Q}(\sqrt{-D_0})$, namely:

$k_2(D)$, the fixed field of $[\bar{A}]^4$;
$\bar{L}'$, the fixed field of $[\bar{B}]$;
$\bar{L}''$, the fixed field of $[\bar{A}^4\bar{B}]$.

$\bar{L}'$ and $\bar{L}''$ are Galois extensions of $\mathbb{Q}$, cyclic of degree 8 over k and having dihedral groups of order 16 as their absolute Galois groups.

Observing $[\bar{A}] \mid k_2(D) = [A]$ and $[\bar{B}] \mid k_2(D) = [B]$, we obtain $\mathrm{Gal}(k_2(D)/\mathbb{Q} = \langle [A], [B], \tau \rangle$. The field $k_2(D)$ possesses 3 subfields of degree 8 containing k, namely

K^*, the fixed field of $[A]^2$;
L', the fixed field of $[B]$;
L'', the fixed field of $[A^2B]$.

K^* is an absolutely abelian extension of type $(2, 2, 2)$, and a simple conductor calculation shows that $K^* = \mathbb{Q}(\sqrt{q}, \sqrt{2}, \sqrt{-1})$, cf. also [**7**]. L' and L'' are Galois extensions of $\mathbb{Q}$, cyclic of degree 4 over k, and having dihedral groups of order 8 as their absolute Galois groups. We are able to distinguish between L' and L'': L' is a subfield of a dihedral field of degree 16 over $\mathbb{Q}$ (e.g., $\bar{L}'$ or $\bar{L}''$), while L'' is not.

Let $L_0 \subset k_2(D)$ be the fixed field of $\langle [A^2], [B] \rangle$; obviously, $k \subset L_0 \subset L^*$, and $L_0 = L' \cap L''$. Since L_0 has an embedding in a dihedral field cyclic over k (namely L'), it follows by [**6**], Satz 22 that

$$L_0 = \begin{cases} \mathbb{Q}(\sqrt{D_0}, \sqrt{2}), & \text{if } q \equiv 7 \bmod 8, \\ \mathbb{Q}(\sqrt{D_0}, \sqrt{-2}), & \text{if } q \equiv 3 \bmod 8. \end{cases}$$

There are two other subfields of K^* which are of interest, namely $k_0 = \mathbb{Q}(\sqrt{|D_0|})$ and $K = kk_0 = \mathbb{Q}(\sqrt{D_0}, \sqrt{-D_0})$. Let $\epsilon_0 > 1$ be the fundamental unit of k_0, and set

$$M = \begin{cases} K(\sqrt[8]{-\epsilon_0}), & \text{if } q \equiv 7 \bmod 8, \\ K(\sqrt[8]{-4\epsilon_0}), & \text{if } q \equiv 3 \bmod 8. \end{cases}$$

The field M was considered in [**4**], Sätze 1, 1a and 1b, where the following facts were proved:

$M/\mathbb{Q}$ is a Galois extension of degree 32, $K^* \subset M$, M/K is cyclic of degree 8, and there exists a subfield $L \subset M$ such that $M = LK$, $L/\mathbb{Q}$ is a Galois extension of degree 16 with a dihedral group as Galois group, $k \subset L$, and L/k is cyclic of degree 8.

Let M_0 be the unique intermediate field between K^* and M. By [**6**], Satz 11, L is contained in a ring class field over k, and since M/k is unramified outside 2, we infer $L \subset k_2(D_s)$ for some $s \geq 2$. It follows from the structure of $\mathcal{H}_2(D_s)$ (determined above) that every cyclic extension of degree 8 over k contained in some $k_2(D_s)$ is already contained in $k_2(4D)$. This implies $L \in \{\bar{L}', \bar{L}''\}$, and consequently $M_0 = L'K$.

The following lemma concerns the splitting type of primes $p \equiv q \bmod 8$ in M.

https://doi.org/10.1017/S0017089500009824 Published online by Cambridge University Press

LEMMA 3. *Let D be a discriminant of type* (I) *or* (II) *and p a rational prime satisfying* $\left(\frac{D_0}{p}\right)=1$ *and* $p\equiv q \bmod 8$. *Then p is inert in k_0 and splits in M_0 into primes of* (*absolute*) *degree* 2. *Moreover, exactly one of the following two assertions holds true*:

1) *p splits completely in L', and the prime divisors of p in M are of degree* 2.
2) *p splits completely in L'', and the prime divisors of p in M are of degree* 4.

Proof. Since $(|D_0|/p)=-(D_0/p)=-1$, p is inert in k_0. For every subfield Ω of M, we denote by $f(\Omega)$ the degree of the prime divisors of p in Ω. We have $f(k)=1$, $f(k_0)=2$, and since $K^*/\mathbb{Q}$ is of type $(2,2,2)$, we infer $f(K^*)=2$. Since $p\equiv 7 \bmod 8$ splits in $\mathbb{Q}(\sqrt{2})$ and $p\equiv 3 \bmod 8$ splits in $\mathbb{Q}(\sqrt{-2})$, we obtain $f(L_0)=1$, and since M_0/L_0 is of type $(2,2)$ and $K^*\subset M_0$, we obtain $f(M_0)=2$ as asserted.

$k_2(D)/L_0$ is an extension of type $(2,2)$ with intermediate fields L', L'' and K^*. Since $f(L_0)=1$ and $f(K^*)=2$, we obtain $f(k_2(D))=2$, and either $f(L')=1$, $f(L'')=2$ or $f(L')=2$, $f(L'')=1$. If $f(L')=1$, then we infer $f(M)=2$, since M/L' is of type $(2,2)$, $M_0\subset M$ and $f(M_0)=2$. If $f(L')=2$, then we infer $f(\bar{L}')=f(\bar{L}'')=4$ since $\bar{L}'/L_0$ and $\bar{L}''/L_0$ are cyclic, and consequently $f(M)=4$ as asserted.

3. Main results.

THEOREM. *Let D be a discriminant of type* (I) *or* (II), *i.e., either*

(I) $D=-256q$, *q prime*, $q\equiv 3 \bmod 4$ *or*

(II) $D=-128q$, *q prime*, $q\equiv 3 \bmod 8$.

Let p be a rational prime satisfying $(D/p)=1$ *and* $p\equiv q \bmod 8$. *Let* $\epsilon_0>1$ *be the fundamental unit of* $k_0=\mathbb{Q}(\sqrt{|D|})$.

i) $-\epsilon_0$ *is a quartic residue modulo p in k_0, and exactly one of the classes A^2B and B represents* $p^{h'(D)}$.

ii) $B\to p^{h'(D)}$ *if and only if* $-\epsilon_0$ *is an octic residue modulo p in k_0.*

Proof. We set

$$\alpha_0=\begin{cases}-\epsilon_0, & \text{if } q\equiv 7 \bmod 8,\\ -4\epsilon_0, & \text{if } q\equiv 3 \bmod 8,\end{cases}$$

whence $M=k(\sqrt[8]{\alpha_0})$ and $M_0=K(\sqrt[4]{\alpha_0})$. The prime p is inert in k_0 and splits in M_0 by Lemma 3, and therefore α_0 is a quartic residue modulo p in k_0.

By Lemma 2, exactly one of the classes B and A^2B represents $p^{h'(D)}$. By Lemma 1, we have $B\to p^{h'(D)}$ if L' is the decomposition field of p in $k_2(D)$, and $A^2B\to p^{h'(D)}$ if L'' is it. By Lemma 3, p splits completely in exactly one of the fields L' and L''. Therefore we obtain $B\to p^{h'(D)}$ if and only if p splits completely in L'. Again by Lemma 3, p splits completely in L' if and only if the prime divisors of p in K split completely in M/K, and since $M=K(\sqrt[8]{\alpha_0})$, this is the case if and only if α_0 is an octic residue modulo p in k_0. Thus we have proved:

α_0 is a quartic modulo p in k_0, and $B\to p^{h'(D)}$ if and only if α_0 is an octic residue modulo p.

To arrive at the assertions of the theorem, we must prove that, for $q\equiv 3 \bmod 8$, 2 is a quartic residue modulo p in k_0 (then 4 is an octic residue); but this is easy, cf. [8], Lemma 2.

Finally we give an interpretation of the criterion stated in the theorem in terms of recurrent sequences.

PROPOSITION. *Let* $m>2$ *be a square-free integer,* $u, v \in \mathbb{N}$, $\epsilon = u + v\sqrt{m} > 1$ *and* $u^2 - mv^2 = 1$. *Let* $p \equiv 3 \bmod 4$ *be a prime satisfying* $(m/p) = -1$. *Define the sequence* $(V_n)_{n\geq 0}$ *by* $V_0 = 2$, $V_1 = -2u$ *and* $V_{n+2} = -2uV_{n+1} - (u^2 - mv^2)V_n$ $(n \geq 0)$.

i) *For any* $n \geq 0$, *we have* $V_n = (-u + v\sqrt{m})^n + (-u - v\sqrt{m})^n$.

ii) $-\epsilon$ *is a quadratic residue modulo* p *in* $\mathbb{Q}(\sqrt{m})$, *and* $V_{(p+1)/2} \equiv \pm 2 \bmod p$.

iii) $-\epsilon$ *is a quartic residue modulo* p *in* $\mathbb{Q}(\sqrt{m})$ *if and only if* $V_{(p+1)/2} \equiv 2 \bmod p$; *in this case we have* $V_{(p+1)/4} \equiv \pm 2 \bmod p$.

iv) *Let* $-\epsilon$ *be a quartic residue modulo* p *in* $\mathbb{Q}(\sqrt{m})$. *Then* $-\epsilon$ *is an octic residue modulo* p *in* $\mathbb{Q}(\sqrt{m})$ *if and only if* $V_{(p+1)/4} \equiv 2 \bmod 4$.

Proof. i) follows by induction.

For the proof of the remaining assertions, let $F = \mathbb{Z}[\sqrt{m}]/(p)$ be the residue class field modulo p, and denote by $\bar{y} \in F$ the residue class of an element $y \in \mathbb{Z}[\sqrt{m}]$. F is a field of p^2 elements, containing the subfield $F_0 = \mathbb{Z}/p\mathbb{Z}$ of rational residue classes. The non-trivial automorphism of F/F_0 is induced by that of $\mathbb{Q}(\sqrt{m})/\mathbb{Q}$ and is given by $(\zeta \mapsto \zeta^p)$. Since $\mathcal{N}(\epsilon) = u^2 - m^2v = 1$, we obtain $\bar{\epsilon}^{1+p} = \bar{1} \in F$, and

$$\bar{V}_n = (-\bar{\epsilon})^n + (-\bar{\epsilon})^{-n} \quad (n \geq 0).$$

Therefore $V_n \equiv \pm 2 \bmod p$ is equivalent with

$$[(-\bar{\epsilon})^n]^2 \mp 2[(-\bar{\epsilon})^n] + \bar{1} = \bar{0},$$

i.e.

$$(-\bar{\epsilon})^n = \pm\bar{1} \in F.$$

Let $\omega \in \mathbb{Z}[\sqrt{m}]$ be a primitive root modulo p, i.e. $F^\times = \langle \bar{\omega} \rangle$, and set $-\bar{\epsilon} = \bar{\omega}^l$ with $l \in \mathbb{N}_0$. Since $\bar{\epsilon}^{1+p} = \bar{1}$, we obtain $l = (p-1)r$ for some $r \in \mathbb{N}$. If $\nu \in \mathbb{N}_0$, $2^\nu \mid p+1$, then $2^{\nu+1} \mid p^2 - 1$, and consequently $-\epsilon$ is a $2^{\nu+1}$th power residue modulo p if and only if $2^\nu \mid r$. If $2^\nu \mid p+1$, then we have

$$(-\bar{\epsilon})^{(p+1)/2^\nu} = \bar{\omega}^{(p^2-1)r/2^\nu} = \bar{1}$$

if and only if $2^\nu \mid r$, and in this case we obtain (provided that $2^{\nu+1} \mid p+1$)

$$(-\bar{\epsilon})^{(p+1)/2^{\nu+1}} = \pm\bar{1}.$$

Applying these arguments for $\nu \in \{0, 1, 2\}$, the assertions of the Proposition follow.

REMARK 1. There are analogues of the proposition above concerning the residuacity character of ϵ or $\pm 2\epsilon$. They also may be used together with the theorem to obtain criteria for the representation by A^2B or B.

REMARK 2. If $m = 3$, then A^2B contains the form $[12, 12, 9]$ and B contains $[3, 0, 64]$; we have $\epsilon_0 = 2 + \sqrt{3}$, and the theorem together with the proposition implies the conjecture of Kaplan and Williams.

REFERENCES

1. D. A. Buell, *Binary quadratic forms* (Springer-Verlag 1989).

2. H. Cohn, *A classical invitation to algebraic numbers and class fields* (Springer-Verlag 1978).

3. S. Gurak, On the representation theory for full decomposable forms, *J. Number Theory* **13** (1981), 421–442.

4. F. Halter-Koch, Quadratische Einheiten als 8. Potenzreste in *Proc. Int. Conf. on Class Numbers and Fundamental Units* (Katata 1986), 1–15.

5. F. Halter-Koch, Einseinheitengruppen und prime Resklassengruppen in quadratischen Zahlkörpern, *J. Number Theory* **4** (1972), 70–77.

6. F. Halter-Koch, Arithmetische Theorie der Normalkörper von 2-Potenzgrad mit Diedergruppe, *J. Number Theory* **3** (1971), 412–443.

7. F. Halter-Koch, Geschlechtertheorie der Ringklassenkörper, *J. Reine Angew. Math.* **250** (1971), 107–108.

8. F. Halter-Koch and N. Ishii, Ring class fields modulo 8 of $\mathbb{Q}(\sqrt{-m})$ and the quartic character of units of $\mathbb{Q}(\sqrt{m})$ for $m \equiv 1 \bmod 8$, *Osaka J. Math.* **26** (1989), 625–646.

9. F. Halter-Koch, P. Kaplan and K. S. Williams, An Artin character and representations of primes by binary quadratic forms II, *Manuscr. Math.* **37** (1982), 357–381.

10. P. Kaplan and K. S. Williams, Representation of primes in arithmetic progressions by binary quadratic forms, *J. Number Theorey*, to appear.

INSTITUT FÜR MATHEMATIK
KARL-FRANZENS-UNIVERSITÄT
HEINRICHSTRASSE 36/IV
A-8010 GRAZ, ÖSTERREICH.