Canad. Math. Bull. Vol. **46** (1), 2003 pp. 39–53

Power Residue Criteria for Quadratic Units and the Negative Pell Equation

Tommy Bülow

Abstract. Let $d > 1$ be a square-free integer. Power residue criteria for the fundamental unit ε_d of the real quadratic fields $\mathbb{Q}(\sqrt{d})$ modulo a prime p (for certain d and p) are proved by means of class field theory. These results will then be interpreted as criteria for the solvability of the negative Pell equation $x^2 - dp^2y^2 = -1$. The most important solvability criterion deals with all d for which $\mathbb{Q}(\sqrt{-d})$ has an elementary abelian 2-class group and $p \equiv 5 \pmod 8$ or $p \equiv 9 \pmod{16}$.

1 Introduction

Let D be a non-square natural number. The problem of deciding whether the negative Pell equation

$$x^2 - Dy^2 = -1, \tag{1}$$

has integral solutions is a classical problem in number theory which is not solved in general. Obvious necessary conditions for the solvability of (1) are that $4 \nmid D$ and that every odd prime factor of D is $\equiv 1 \pmod 4$; they are *not* sufficient.

Consider two indefinite integral binary quadratic forms of positive discriminant: $f(x, y) = ax^2 + bxy + cy^2$ and $g(x, y) = a'x^2 + b'xy + c'y^2$. Then f and g are called equivalent if there is a matrix $A = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \in \mathrm{GL}_2(\mathbb{Z})$ such that $f(x, y) = g(\alpha x + \beta y, \gamma x + \delta y)$; if this holds and $A \in \mathrm{SL}_2(\mathbb{Z})$, then f and g are called *properly* equivalent (these matters where studied by Gauss). The discriminant of f is $b^2 - 4ac$. If we consider forms of fixed positive non-square discriminant D, then it is known that

$$\text{proper equivalence} = \text{equivalence} \iff x^2 - Dy^2 = -4 \text{ is solvable.}$$

If $4 \nmid D$, then these two statements are true if and only if $x^2 - Dy^2 = -1$ is solvable.

Many mathematicians have made sporadic contributions to the problem about the solvability of (1). Fermat and Euler were some of the first to study the equation systematically. First, suppose that D is square-free. Dirichlet [2] proved (by rather elementary means) certain sufficient conditions for solvability (expressed in terms of the quadratic or biquadratic residue character of the prime factors of D). More recent results can be found in [3], [10], [11], [12], [13].

Received by the editors April 27, 2001; revised August 19, 2001.
AMS subject classification: 11R11, 11R27.

We shall consider the case where D is *not* square-free. Let $d > 1$ be a square-free integer and let $k > 1$ be a an odd integer. The equation (1) with D not square-free (and, of course, $4 \nmid D$) can be written

$$x^2 - dk^2y^2 = -1. \tag{2}$$

We note that the problem in question is that of deciding whether the norm of the fundamental unit of the order of conductor k in $\mathbb{Q}(\sqrt{d})$ is 1 or -1. This has consequences for the structure of the corresponding ring class fields. For the class field theory to be used we refer to [1] or [5].

We mention (without proof) another formulation of the problem in terms of class field theory: Consider the two ideal groups in $K := \mathbb{Q}(\sqrt{d})$ (where $A_{(k)}(K)$ denotes the group of fractional ideals in K relatively prime to k):

$$H' := \left\{ (\alpha) \in A_{(k)}(K) \mid \exists\, r \in \mathbb{Q} : \alpha \equiv r \pmod{(k)} \right\} \quad \text{and}$$
$$H'' := \left\{ (\alpha) \in A_{(k)}(K) \mid \exists\, r \in \mathbb{Q} : \alpha \equiv r \pmod{(k)\infty} \right\};$$

(k) (resp. $(k)\infty$) is clearly a congruence module for H' (resp. H''); ∞ is the divisor of K which is the product of the real embeddings of K. Let L' (resp. L'') be the abelian extension of K corresponding to H' (resp. H''). By definition of infinite ramification, $L' \subseteq \mathbb{R}$. It is also clear that $H' \supseteq H''$. Then the following is true:

Proposition 1 *The following three conditions are equivalent (for $2 \nmid k$).*

(1) $x^2 - dk^2y^2 = -1$ *is solvable.*
(2) $H' = H''$.
(3) $L'' \subseteq \mathbb{R}$.

When studying the existence of integral solutions to (2) one can, as is well-known, assume that k is a prime number $p \equiv 1 \pmod 4$. Of course, one can assume that (2) with $k = 1$ has a solution. We shall also assume that $p \nmid d$. It is not hard to show that if $(\frac{d}{p}) = -1$ and if $x^2 - dy^2 = -1$ is solvable, then $x^2 - dp^2y^2 = -1$ is also solvable.

The remaining case, $(\frac{d}{p}) = 1$, is still not completely settled. Below we use class field theory to prove some results concerning this case.

Let $\varepsilon_d > 1$ be the fundamental unit of the real quadratic field $\mathbb{Q}(\sqrt{d})$. When the norm of ε_d is -1, the solvability of (2) with k being a prime number $p \equiv 1 \pmod 4$ is closely related to the power residue character of ε_d modulo p. In [7], the following lemma is proved in an elementary way.

Lemma 1 *Let $d > 1$ be a square-free integer. Let the fundamental unit ε_d of $\mathbb{Q}(\sqrt{d})$ have norm -1 and let $p \equiv 1 \pmod 4$ be a prime number with $(\frac{d}{p}) = 1$. Suppose that $2^\lambda \parallel p - 1$. Then*

$$x^2 - dp^2y^2 = -1 \text{ is solvable} \iff (\varepsilon_d)^{\frac{p-1}{2^{\lambda-1}}} \equiv -1 \pmod p \quad (\text{in } \mathcal{O}_{\mathbb{Q}(\sqrt{d})}).$$

If c is an integer not divisible by the odd prime p and the Legendre symbol $(\frac{c}{p})$ has the value 1, then we define the symbol $(\frac{c}{p})_4$ to be be 1 or -1 according as c is or is not a fourth power modulo p. If $(\frac{d}{p}) = 1$, then we can interpret ε_d as an integer modulo p and if the norm $N(\varepsilon_d)$ of ε_d is 1 or if $N(\varepsilon_d) = -1$ and $p \equiv 1 \pmod 4$, the symbol $(\frac{\varepsilon_d}{p})$ is well-defined. When there is no risk of ambiguity, we define, recursively, the symbol $(\frac{\varepsilon_d}{p})_{2^{t+1}} = 1$ (resp. $= -1$) to mean that $(\frac{\varepsilon_d}{p})_{2^t} = 1$ and ε_d is (resp. is not) a 2^{t+1}-th power modulo p. For our purposes it will be sufficient to know that if $N(\varepsilon_d) = 1$ or if $N(\varepsilon_d) = -1$ and $p \equiv 1 \pmod 8$, the symbol $(\frac{\varepsilon_d}{p})_4$ is well defined.

Observation 1 Let $p \equiv 1 \pmod{2^\lambda}$ $(\lambda = 2, 3)$ be a prime number with $(\frac{d}{p}) = 1$ and let $\mathfrak{p}$ be one of the two prime ideals in $\mathbb{Q}(\sqrt{-d})$ above p. Then

$$\left(\frac{\varepsilon_d}{p}\right)_{2^{\lambda-1}} = 1 \Longleftrightarrow (\varepsilon_d)^{\frac{p-1}{2^{\lambda-1}}} \equiv 1 \pmod p$$
$$\Longleftrightarrow \mathfrak{p} \text{ splits totally in } \mathbb{Q}(\sqrt[2^{\lambda-1}]{\varepsilon_d}, i),$$

by Theorem 119 in [6]. In particular, we immediately have (*cf.* Lemma 1):

A) $p \equiv 5 \pmod 8$:

$$x^2 - dp^2y^2 = -1 \text{ is solvable } \Longleftrightarrow \left(\frac{\varepsilon_d}{p}\right) = -1;$$

B) $p \equiv 9 \pmod{16}$:

$$x^2 - dp^2y^2 = -1 \text{ is solvable } \Longleftrightarrow \left(\frac{\varepsilon_d}{p}\right)_4 = -1;$$

C) $p \equiv 1 \pmod{16}$:

$$x^2 - dp^2y^2 = -1 \text{ is solvable } \Longrightarrow \left(\frac{\varepsilon_d}{p}\right)_4 = 1.$$

2 Some Related Results in the Literature

We describe some of the known results dealing with the power residue criteria for ε_d or the solvability of (2) with k being a prime p. They are almost all expressed in terms of one or two representations of powers of p by binary quadratic forms.

Reference [4] contains several power residue criteria for ε_d being a 2^t-th power residue ($t = 1, 2, 3$) for special classes of d. A typical example is Potenzrestkriterium 1 in [4]:

Theorem 1 *Let $d \equiv 7 \pmod 8$, let the prime divisors q of m be $\equiv \pm 1 \pmod 8$, let the class group of $\mathbb{Q}(\sqrt{-d})$ have no invariant divisible by 4, let m be the odd part of the class number of $\mathbb{Q}(\sqrt{-d})$, let $p \equiv 1 \pmod 8$ be a prime number such that $(\frac{q}{p}) = 1$ for every prime factor q of d. Then $p^m = s^2 + 16dv^2$, $s, v \in \mathbb{Z}$, $(\frac{\varepsilon_d}{p}) = 1$ and $(\frac{\varepsilon_d}{p})_4 = (-1)^v$. If $p \equiv 1 \pmod{16}$ and $(\frac{\varepsilon_d}{p})_4 = 1$, i.e., $p^m = s^2 + 64d(v_1)^2$, $s, v_1 \in \mathbb{Z}$, then $(\frac{\varepsilon_d}{p})_8 = (-1)^{v_1}$.*

https://doi.org/10.4153/CMB-2003-004-1 Published online by Cambridge University Press

We refer to [4] for references to older power residue criteria in the literature.

Let us now turn to the case which interests us in this paper, namely $N(\varepsilon_d) = -1$ (*i.e.*, $x^2 - dy^2 = -1$ is solvable), $p \equiv 1 \pmod 4$ and $(\frac{d}{p}) = 1$. This is assumed in the rest of this section.

The old paper [9] contains the following criterion:

Theorem 2 *Let $p \equiv 1 \pmod 8$ be a prime represented by $p = s^2 + 2v^2$; a necessary condition for the solvability of $x^2 - 2p^2y^2 = -1$ is that $8|v$; for $p \equiv 9 \pmod{16}$ this condition is also sufficient.*

Remark 1 Let $p \equiv 1 \pmod 8$ be a prime. Then (by Gauss) 2 is a biquadratic residue modulo p if and only if $p = x^2 + 64y^2$. If $p \equiv 1 \pmod{16}$, then this is equivalent to $p = s^2 + 128v^2$.

In [8], Theorem 2 was extended to a similar criterion when $p \equiv 17 \pmod{32}$:

Theorem 3 *Let $p \equiv 1 \pmod{16}$ be a prime satisfiying the necessary condition of Theorem 2, i.e., representable by the form $p = s^2 + 128v_1^2$ and hence also by $p = x^2 + 64y^2$. Then a necessary condition for the solvability of $x^2 - 2p^2y^2 = -1$ is that $y + v_1 \equiv \frac{p-1}{16} \pmod 2$; for $p \equiv 17 \pmod{32}$ this condition is also sufficient.*

In [7], a necessary and sufficient condition was given in the case $d = q \equiv 1 \pmod 4$ a prime and $p \equiv 5 \pmod 8$. For example, for $q \equiv 5 \pmod 8$:

Theorem 4 *Let $q \equiv 5 \pmod 8$ be a prime. Let p be a prime $\equiv 1 \pmod 4$ with $(\frac{d}{p}) = 1$. Then $p^{h/2} = u^2 + qv^2$, h being the class number of $\mathbb{Q}(\sqrt{-q})$.*

A necessary condition for the solvability of $x^2 - qp^2y^2 = -1$ is that $\frac{p-1}{4} + v$ is even; for $p \equiv 5 \pmod 8$ this condition is also sufficient.

In this paper, generalized criteria of the same type as the three previous ones are obtained. Certain (infinite) classes of not necessarily prime d will be covered.

3 The Main Results

We first fix some relevant notation for the subsequent discussion.

Let $d > 1$ be a square-free integer. Let $p_1, \dots, p_r$ be the odd prime factors of d. Let $\varepsilon_d = \frac{u+t\sqrt{d}}{2} > 1$ ($u, t \in \mathbb{Z}$) be the fundamental unit of $\mathbb{Q}(\sqrt{d})$. Assume that $N(\varepsilon_d) = -1$. It is readily verified that $(\frac{u}{p_i}) = 1$. If u is a biquadratic residue $\pmod{p_i}$, we say that p_i is of type I; otherwise, p_i is of type II. Let β be the number of p_i of type II. The symbol $\wedge$ will denote the logical 'and'; the symbol $\vee$ is the logical 'or'.

Proofs of the results in this section can be found in the subsequent section.

Lemma 2 *Let $d > 1$ be a square-free integer and assume that $N(\varepsilon_d) = -1$ (i.e., $x^2 - dy^2 = -1$ is solvable). Let $p \equiv 1 \pmod 4$ be a prime number such that*

https://doi.org/10.4153/CMB-2003-004-1 Published online by Cambridge University Press

$(\frac{d}{p}) = 1$; let $\mathfrak{p}$ be one of the two prime ideals in $\mathbb{Q}(\sqrt{-d})$ above p. Let the class number of $\mathbb{Q}(\sqrt{-d})$ be $h\big(\mathbb{Q}(\sqrt{-d})\big) = 2^z m$, $2 \nmid m$.

For $d \equiv 5 \pmod 8$ or $2|d$: Assume that $\mathfrak{p}^{2m}$ is a principal ideal. For $d \equiv 1 \pmod 8$: Assume that $\mathfrak{p}^m$ is a principal ideal. Then the following assertions hold:

(1) $d \equiv 5 \pmod 8$*: There is a relation*

$$p^{m_0} = d_1 s^2 + d_2 v^2, \quad s, v \in \mathbb{Z} \setminus \{0\}, d_1, d_2 \in \mathbb{N}, d_1 d_2 = d, p_r \nmid d_1,$$

with m_0 minimal (this implies $m_0|m$). Put

$$\Sigma_1 := \text{the number of prime factors of } d_1 \text{ of type II (with respect to } d\text{)}.$$

(2) $2|d$*: There is a relation*

$$p^{m_0} = d_1 s^2 + d_2 v^2, \quad s, v \in \mathbb{Z} \setminus \{0\}, d_1, d_2 \in \mathbb{N}, d_1 d_2 = d, 2 \nmid d_1,$$

with m_0 minimal (this implies $m_0|m$). Put

$$\Sigma_2 := \text{the number of prime factors of } d_1 \text{ of type II (with respect to } d\text{)}.$$

(3) $d \equiv 1 \pmod 8$*: $\exists\, s, v \in \mathbb{Z} \setminus \{0\}$, minimal odd $n_0 \in \mathbb{N}$: $p^{n_0} = s^2 + dv^2$.*

And this is equivalent to $\mathfrak{p}^m$ being a principal ideal.

Theorem 5 *Let the assumptions and the notation be as in Lemma 2. Then*

$$\left(\frac{\varepsilon_d}{p}\right) = (-1)^{\frac{p-1}{4} + \frac{sv}{2}}.$$

Remark 2 Clearly, if $2|d$, then this can be written as $(\frac{\varepsilon_d}{p}) = (-1)^{\frac{p-1}{4} + \frac{v}{2}}$; and if $d \equiv 1 \pmod 8$, then we have $(\frac{\varepsilon_d}{p}) = 1$.

Theorem 6 *Let the assumptions and the notation be as in Lemma 2. Let $d \equiv 5 \pmod 8$. Let $p \equiv 1 \pmod 8$ and write $p = a^2 + 16b^2$, $a, b \in \mathbb{Z}$. Then for*

(i) $2|\beta$:

$$\left(\frac{\varepsilon_d}{p}\right)_4 = 1 \iff \Big(2|b \wedge \big((2|\Sigma_1 \wedge 8|sv) \vee (2 \nmid \Sigma_1 \wedge 4 \parallel sv)\big)\Big) \\ \vee \Big(2 \nmid b \wedge \big((2|\Sigma_1 \wedge 4 \parallel sv) \vee (2 \nmid \Sigma_1 \wedge 8|sv)\big)\Big);$$

(ii) $2 \nmid \beta$:

$$\left(\frac{\varepsilon_d}{p}\right)_4 = 1 \iff \\ \Big(2|b \wedge \Big(\big(2|\Sigma_1 \wedge (4 \parallel s \vee 8|v)\big) \vee \big(2 \nmid \Sigma_1 \wedge (8|s \vee 4 \parallel v)\big)\Big)\Big) \\ \vee \Big(2 \nmid b \wedge \Big(\big(2|\Sigma_1 \wedge (8|s \vee 4 \parallel v)\big) \vee \big(2 \nmid \Sigma_1 \wedge (4 \parallel s \vee 8|v)\big)\Big)\Big).$$

https://doi.org/10.4153/CMB-2003-004-1 Published online by Cambridge University Press

Theorem 7 *Let the assumptions and the notation be as in Lemma 2. Let* $2|d$. *Let* $p \equiv 1 \pmod 8$ *and write* $p = a^2 + 16b^2$, $a, b \in \mathbb{Z}$. *Then*

$$\left(\frac{\varepsilon_d}{p}\right)_4 = 1 \iff \Big(2|b \wedge \big((2|\Sigma_2 \wedge 8|v) \vee (2 \nmid \Sigma_2 \wedge 4 \parallel v)\big)\Big) \vee \Big(2 \nmid b \wedge \big((2|\Sigma_2 \wedge 4 \parallel v) \vee (2 \nmid \Sigma_2 \wedge 8|v)\big)\Big).$$

Theorem 8 *Let the assumptions and the notation be as in Lemma 2. Let* $d \equiv 1 \pmod 8$. *Let* $p \equiv 1 \pmod 8$ *and write* $p = a^2 + 16b^2$, $a, b \in \mathbb{Z}$. *Then for*

(i) $2|\beta$:

$$\left(\frac{\varepsilon_d}{p}\right)_4 = 1 \iff (2|b \wedge 8|sv) \vee (2 \nmid b \wedge 8 \nmid sv);$$

(ii) $2 \nmid \beta$:

$$\left(\frac{\varepsilon_d}{p}\right)_4 = 1 \iff \big(2|b \wedge (4 \parallel s \vee 8|v)\big) \vee (2 \nmid b \wedge 4 \not\parallel s \wedge 8 \nmid v).$$

When Theorems 6, 7 and 8 are interpreted in terms of the solvability of the negative Pell equation $x^2 - dp^2y^2 = -1$ (*cf.* Observation 1), we easily deduce the following three theorems.

Theorem 9 *Let the assumptions and the notation be as in Lemma 2. Let* $d \equiv 5 \pmod 8$. *If* $p \equiv 1 \pmod 8$, *we write* $p = a^2 + 16b^2$, $a, b \in \mathbb{Z}$. *Then for*

(A) $p \equiv 5 \pmod 8$:

$$x^2 - dp^2y^2 = -1 \text{ is solvable } \iff 4|sv.$$

(B) $p \equiv 9 \pmod{16}$:

(i) $2|\beta$:

$$x^2 - dp^2y^2 = -1 \text{ is solvable } \iff \Big(2 \nmid b \wedge \big((2|\Sigma_1 \wedge 8|sv) \vee (2 \nmid \Sigma_1 \wedge 4 \parallel sv)\big)\Big) \vee \Big(2|b \wedge \big((2|\Sigma_1 \wedge 4 \parallel sv) \vee (2 \nmid \Sigma_1 \wedge 8|sv)\big)\Big);$$

(ii) $2 \nmid \beta$:

$$x^2 - dp^2y^2 = -1 \text{ is solvable } \iff \Big(2 \nmid b \wedge \Big(\big(2|\Sigma_1 \wedge (4 \parallel s \vee 8|v)\big) \vee \big(2 \nmid \Sigma_1 \wedge (8|s \vee 4 \parallel v)\big)\Big)\Big) \vee \Big(2|b \wedge \Big(\big(2|\Sigma_1 \wedge (8|s \vee 4 \parallel v)\big) \vee \big(2 \nmid \Sigma_1 \wedge (4 \parallel s \vee 8|v)\big)\Big)\Big).$$

https://doi.org/10.4153/CMB-2003-004-1 Published online by Cambridge University Press

(C) $p \equiv 1 \pmod{16}$:

(i) $2|\beta$:

$$x^2 - dp^2y^2 = -1 \text{ is solvable } \Longrightarrow \Big(2|b \wedge \big((2|\Sigma_1 \wedge 8|sv) \vee (2 \nmid \Sigma_1 \wedge 4 \parallel sv)\big)\Big) \vee \Big(2 \nmid b \wedge \big((2|\Sigma_1 \wedge 4 \parallel sv) \vee (2 \nmid \Sigma_1 \wedge 8|sv)\big)\Big);$$

(ii) $2 \nmid \beta$:

$$x^2 - dp^2y^2 = -1 \text{ is solvable } \Longrightarrow \bigg(2|b \wedge \Big(\big(2|\Sigma_1 \wedge (4 \parallel s \vee 8|v)\big) \vee \big(2 \nmid \Sigma_1 \wedge (8|s \vee 4 \parallel v)\big)\Big)\bigg) \vee \bigg(2 \nmid b \wedge \Big(\big(2|\Sigma_1 \wedge (8|s \vee 4 \parallel v)\big) \vee \big(2 \nmid \Sigma_1 \wedge (4 \parallel s \vee 8|v)\big)\Big)\bigg).$$

Theorem 10 *Let the assumptions and the notation be as in Lemma 2. Let $2|d$. If $p \equiv 1 \pmod 8$, we write $p = a^2 + 16b^2$, $a, b \in \mathbb{Z}$. Then for*

(A) $p \equiv 5 \pmod 8$:

$$x^2 - dp^2y^2 = -1 \text{ is solvable } \Longleftrightarrow 2 \not\parallel v;$$

(B) $p \equiv 9 \pmod{16}$:

$$x^2 - dp^2y^2 = -1 \text{ is solvable } \Longleftrightarrow \Big(2 \nmid b \wedge \big((2|\Sigma_2 \wedge 8|v) \vee (2 \nmid \Sigma_2 \wedge 4 \parallel v)\big)\Big) \vee \Big(2|b \wedge \big((2|\Sigma_2 \wedge 4 \parallel v) \vee (2 \nmid \Sigma_2 \wedge 8|v)\big)\Big);$$

(C) $p \equiv 1 \pmod{16}$:

$$x^2 - dp^2y^2 = -1 \text{ is solvable } \Longrightarrow \Big(2|b \wedge \big((2|\Sigma_2 \wedge 8|v) \vee (2 \nmid \Sigma_2 \wedge 4 \parallel v)\big)\Big) \vee \Big(2 \nmid b \wedge \big((2|\Sigma_2 \wedge 4 \parallel v) \vee (2 \nmid \Sigma_2 \wedge 8|v)\big)\Big).$$

Theorem 11 *Let the assumptions and the notation be as in Lemma 2. Let $d \equiv 1 \pmod 8$. If $p \equiv 1 \pmod 8$, we write $p = a^2 + 16b^2$, $a, b \in \mathbb{Z}$. Then for*

(A) $p \equiv 5 \pmod 8$:

$$x^2 - dp^2y^2 = -1 \text{ is not solvable.}$$

https://doi.org/10.4153/CMB-2003-004-1 Published online by Cambridge University Press

(B) $p \equiv 9 \pmod{16}$:

(a) $2|\beta$:

$$x^2 - dp^2y^2 = -1 \text{ is solvable } \iff (2 \nmid b \wedge 8|sv) \vee (2|b \wedge 8 \nmid sv).$$

(b) $2 \nmid \beta$:

$$x^2 - dp^2y^2 = -1 \text{ is solvable } \iff \big(2 \nmid b \wedge (4 \parallel s \vee 8|v)\big) \vee (2|b \wedge 4 \nparallel s \wedge 8 \nmid v).$$

(C) $p \equiv 1 \pmod{16}$:

(a) $2|\beta$:

$$x^2 - dp^2y^2 = -1 \text{ is solvable } \Longrightarrow (2|b \wedge 8|sv) \vee (2 \nmid b \wedge 8 \nmid sv).$$

(b) $2 \nmid \beta$:

$$x^2 - dp^2y^2 = -1 \text{ is solvable } \Longrightarrow \big(2|b \wedge (4 \parallel s \vee 8|v)\big) \vee (2 \nmid b \wedge 4 \nparallel s \wedge 8 \nmid v).$$

Remark 3 If $x^2 - dy^2 = -1$ has a solution and the 2-class group of $\mathbb{Q}(\sqrt{-d})$ is elementary abelian, then the condition about $\mathfrak{p}^{2m}$ being principal is clearly fulfilled for all p and it is not hard to show that $d \equiv 5 \pmod 8$ or $2|d$. We note that Theorem 10 is a generalization of Theorem 2.

Example 1 Let $d = 85 = 5 \cdot 17 \equiv 5 \pmod 8$. Then: $\varepsilon_{85} = \frac{9+\sqrt{85}}{2}$; $N(\varepsilon_{85}) = -1$; $\beta = 2$. The class number is $h\big(\mathbb{Q}(\sqrt{-85})\big) = 4$, so the class group of $\mathbb{Q}(\sqrt{-85})$ is $(\mathbb{Z}/2)^2$ which implies that Theorems 6 and 9 cover all prime numbers $p \equiv 1 \pmod 4$ for which 85 is a quadratic residue (and we have $m_0 = 1$). For example, for the prime $p = 1481 = 35^2 + 16 \cdot 4^2 = 11^2 + 85 \cdot 4^2 \equiv 9 \pmod{16}$: $(\frac{85}{1481}) = 1$; $\Sigma_1 = 0$;

$$\left(\frac{\varepsilon_{85}}{1481}\right) = (-1)^{\frac{1481-1}{4} + \frac{11 \cdot 4}{2}} = 1; \quad \left(\frac{\varepsilon_{85}}{1481}\right)_4 = -1;$$

$$x^2 - 85 \cdot 1481^2 y^2 = -1 \text{ is solvable.}$$

Example 2 Let $d = 10 = 2 \cdot 5$. $\varepsilon_{10} = 3 + \sqrt{10}$; $N(\varepsilon_{10}) = -1$; $h\big(\mathbb{Q}(\sqrt{-10})\big) = 2$. So Theorems 7 and 10 cover all prime numbers $p \equiv 1 \pmod 4$ for which $(\frac{10}{p}) = 1$ (and $m_0 = 1$). For example, for the prime $p = 809 = 5^2 + 16 \cdot 7^2 = 13^2 + 10 \cdot 8^2 \equiv 9 \pmod{16}$: $(\frac{10}{809}) = 1$; $\Sigma_2 = 0$;

$$\left(\frac{\varepsilon_{10}}{809}\right) = (-1)^{\frac{809-1}{4} + \frac{8}{2}} = 1; \quad \left(\frac{\varepsilon_{10}}{809}\right)_4 = -1; \quad x^2 - 10 \cdot 809^2 y^2 = -1 \text{ is solvable.}$$

Example 3 Let $d = 145 = 5 \cdot 29 \equiv 1 \pmod 8$. $\varepsilon_{145} = 12 + \sqrt{145}$; $N(\varepsilon_{145}) = -1$; $\beta = 1$; $h\big(\mathbb{Q}(\sqrt{-145})\big) = 8$. So Theorems 8 and 11 cover all prime numbers $p = s^2 + 145v^2$. For example, for the prime $p = 2441 = 29^2 + 16 \cdot 10^2 = 11^2 + 145 \cdot 4^2 \equiv 9 \pmod{16}$:

$$\left(\frac{\varepsilon_{145}}{2441}\right) = 1; \quad \left(\frac{\varepsilon_{145}}{2441}\right)_4 = -1; \quad x^2 - 145 \cdot 2441^2 y^2 = -1 \text{ is solvable.}$$

https://doi.org/10.4153/CMB-2003-004-1 Published online by Cambridge University Press

4 Proofs of the Main Results

In this section we prove the results (and work with the assumptions and notation) from the previous section. Put $\varepsilon = \varepsilon_d$.

The extension $\mathbb{Q}(\sqrt{\varepsilon}, i)/\mathbb{Q}(\sqrt{-d})$ is Galois with Galois group $\mathbb{Z}/4$; but the extension $\mathbb{Q}(\sqrt[4]{\varepsilon}, i)/\mathbb{Q}(\sqrt{-d})$ is not Galois for $d \neq 2$. From now on, we assume that $d \neq 2$, *cf.* Remark 3. The extension $\mathbb{Q}(\sqrt[4]{2\varepsilon}, i)/\mathbb{Q}(\sqrt{-d})$ is Galois with Galois group $\mathbb{Z}/8$. By well-known ramification theory we have for a prime ideal $\mathfrak{p}$ in $\mathbb{Q}(\sqrt{-d})$ above p:

$$
\begin{aligned}
&\mathfrak{p} \text{ splits totally in } \mathbb{Q}(\sqrt[4]{\varepsilon}, i) \iff \\
&\quad \mathfrak{p} \text{ splits totally in } \mathbb{Q}(\sqrt{\varepsilon}, i) \wedge \\
&\qquad \left(\left(\left(\frac{2}{p}\right)_4 = 1 \wedge \mathfrak{p} \text{ splits totally in } \mathbb{Q}(\sqrt[4]{2\varepsilon}, i) \right) \right. \\
&\qquad\quad \left. \vee \left(\left(\frac{2}{p}\right)_4 = -1 \wedge \mathfrak{p} \text{ does not split totally in } \mathbb{Q}(\sqrt[4]{2\varepsilon}, i) \right) \right).
\end{aligned}
$$

The solvability of our equation is, therefore, a question of the splitting of $\mathfrak{p}$ in *abelian* extensions of $\mathbb{Q}(\sqrt{-d})$; hence we can apply class field theory.

Clearly, in the extensions $\mathbb{Q}(\sqrt{\varepsilon}, i)/\mathbb{Q}(\sqrt{-d})$ and $\mathbb{Q}(\sqrt[4]{2\varepsilon}, i)/\mathbb{Q}(\sqrt{-d})$ there can only be ramification above 2. Let $A_{(2)}$ be the group of fractional ideals in $\mathbb{Q}(\sqrt{-d})$ relatively prime to 2. Let (in the sense of class field theory) $H_{-1}, H_\varepsilon, H_{2\varepsilon}, H \subseteq A_{(2)}$ be the ideal groups in $\mathbb{Q}(\sqrt{-d})$ where

(a) H_{-1} corresponds to $\mathbb{Q}(\sqrt{d}, i)$;
(b) H_ε corresponds to $\mathbb{Q}(\sqrt{\varepsilon}, i)$;
(c) $H_{2\varepsilon}$ corresponds to $\mathbb{Q}(\sqrt{2\varepsilon}, i)$;
(d) H corresponds to $\mathbb{Q}(\sqrt[4]{2\varepsilon}, i)$.

As a prime ideal in a base field splits totally in an abelian extension if and only if it is in the corresponding ideal group, it is our task to describe the prime ideals in H_ε and in H.

Proposition 2 *Let $\mathfrak{p}_0$ be the prime ideal in $\mathbb{Q}(\sqrt{-d})$ above the odd prime factor n of d. Then*

(1) $\mathfrak{p}_0 \in H_{2\varepsilon}$.
(2) $(\sqrt{-d}) \in H_{2\varepsilon}$ *if d is odd.*
(3) $\mathfrak{p}_0 \in H \Leftrightarrow n$ *is of type I.*
(4) *For d odd:* $(\sqrt{-d}) \in H \Leftrightarrow 2|\beta$.
(5) $\mathfrak{p}_0 \in H_\varepsilon \Leftrightarrow n \equiv 1 \pmod 8$.
(6) $(\sqrt{-d}) \in H_\varepsilon \Leftrightarrow d \equiv 1 \pmod 8$.

https://doi.org/10.4153/CMB-2003-004-1 Published online by Cambridge University Press

Proof (1) Let $\mathfrak{p}_1$ be the prime ideal in $\mathbb{Q}(\sqrt{d})$ above n. We have:

$$\begin{aligned}\mathfrak{p}_0 \in H_{2\varepsilon} &\iff \mathfrak{p}_0 \text{ splits totally in } \mathbb{Q}(\sqrt{2\varepsilon}, i)\\ &\iff \mathfrak{p}_1 \text{ splits totally in } \mathbb{Q}(\sqrt{2\varepsilon})\\ &\iff x^2 \equiv u + t\sqrt{d} \pmod{\mathfrak{p}_1} \text{ is solvable in } \mathcal{O}_{\mathbb{Q}(\sqrt{d})}\\ &\iff u^{\frac{N(\mathfrak{p}_1)-1}{2}} \equiv 1 \pmod{\mathfrak{p}_1}\\ &\iff \Big(\frac{u}{n}\Big) = 1.\end{aligned}$$

And this last statement is true.

(2) Follows from (1) and the fact that $(\sqrt{-d})$ is the product of the prime ideals in $\mathbb{Q}(\sqrt{-d})$ above the prime factors of d

(3) Let (*cf.* (1)) $\mathfrak{p}_2$ be one (of the two) prime ideal(s) in $\mathbb{Q}(\sqrt{2\varepsilon})$ above n. We have:

$$\begin{aligned}\mathfrak{p}_0 \in H &\iff \mathfrak{p}_0 \text{ splits totally in } \mathbb{Q}(\sqrt[4]{2\varepsilon}, i)\\ &\iff \mathfrak{p}_2 \text{ splits totally in } \mathbb{Q}(\sqrt[4]{2\varepsilon})\\ &\iff \Big(\sqrt{u + t\sqrt{d}}\Big)^{\frac{N(\mathfrak{p}_2)-1}{2}} \equiv 1 \pmod{\mathfrak{p}_2}\\ &\iff u^{\frac{n-1}{4}} \equiv 1 \pmod{n}\\ &\iff n \text{ is of type I.}\end{aligned}$$

(4) Since $\mathfrak{p}_0 \in H_{2\varepsilon}$, this is an immediate consequence of (3) and the fact that $|H_{2\varepsilon}/H| = 2$.

(5) and (6) are proved by similar means. ■

Lemma 3 *Let $p \equiv 1 \pmod 4$ be a prime number. Let $2\varepsilon = u + t\sqrt{d}$. Then*

(1) *For $p|d$:*

$$(p) \in H.$$

(2) *For $(\frac{d}{p}) = 1$:*

$$(p) \in H.$$

(3) *For $(\frac{d}{p}) = -1$:*

$$(u + t\sqrt{d})^{\frac{p^2-1}{4}} \equiv 1 \pmod{p} \quad \textit{in } \mathcal{O}_{\mathbb{Q}(\sqrt{d})} \Longrightarrow (p) \in H.$$

Proof (1) and (3) are easy, *cf.* (the proof of) Proposition 2.

(2) $(\frac{d}{p}) = 1$: Let $\mathfrak{p}$ be a prime ideal in $\mathbb{Q}(\sqrt{-d})$ above p, let $\mathfrak{p}'$ be the conjugate ideal. As $\mathfrak{p}$ and $\mathfrak{p}'$ split totally in $\mathbb{Q}(\sqrt{d}, i)$, the inertial degrees of $\mathfrak{p}$ and $\mathfrak{p}'$ in $L := \mathbb{Q}(\sqrt[4]{2\varepsilon}, i)$ divide 4. So if we put $K := \mathbb{Q}(\sqrt{-d})$, then we have (for the Artin symbols)

$$\operatorname{ord}\Big(\Big(\frac{L/K}{\mathfrak{p}}\Big)\Big) = \operatorname{ord}(\mathfrak{p}H) = \operatorname{ord}(\mathfrak{p}'H) = \operatorname{ord}\Big(\Big(\frac{L/K}{\mathfrak{p}'}\Big)\Big) \;\Big|\; 4.$$

If $\operatorname{ord}(\mathfrak{p}H) = \operatorname{ord}(\mathfrak{p}'H) = 1$, then $(p) = \mathfrak{p}\mathfrak{p}' \in H$. If $\operatorname{ord}(\mathfrak{p}H) = \operatorname{ord}(\mathfrak{p}'H) = 2$, then (since $A_{(2)}/H \simeq \mathbb{Z}/8$) $(p) \in (p)H = (\mathfrak{p}H)(\mathfrak{p}'H) = H$.

Consider the remaining case: $\operatorname{ord}(\mathfrak{p}H) = \operatorname{ord}(\mathfrak{p}'H) = 4$; then

$$\Big(\frac{L/K}{\mathfrak{p}}\Big), \Big(\frac{L/K}{\mathfrak{p}'}\Big) \in \operatorname{Gal}\big(L/\mathbb{Q}(\sqrt{d}, i)\big).$$

So $(\frac{L/K}{\mathfrak{p}})$ and $(\frac{L/K}{\mathfrak{p}'})$ are determined by their values on $\sqrt[4]{2\varepsilon}$. It is readily verified that

$$\Big(\frac{L/K}{\mathfrak{p}}\Big) \circ \Big(\frac{L/K}{\mathfrak{p}'}\Big)(\sqrt[4]{2\varepsilon}) = \sqrt[4]{2\varepsilon}.$$

Hence, by the isomorphism $A_{(2)}/H \simeq \operatorname{Gal}(L/K)$ (induced by the Artin map),

$$(p) \in (p)H = (\mathfrak{p}H)(\mathfrak{p}'H) = H. \qquad \blacksquare$$

Let $S_{\mathfrak{M}}$ denote the ray class group modulo the divisor $\mathfrak{M}$ in $\mathbb{Q}(\sqrt{-d})$. We are now able to determine the principal ideals in the ideal groups:

Theorem 12 *The subgroups of principal ideals in the ideal groups H_{-1}, H_ε, $H_{2\varepsilon}$, H are as follows (where β is the number of odd prime factors of d of type II):*

(1) $d \equiv 1 \pmod 4$*:*

$$H_{-1} \cap S_{(1)} = A_{(2)} \cap S_{(1)};$$

$$H_\varepsilon \cap S_{(1)} = \begin{cases} A_{(2)} \cap S_{(1)}, & \text{if } d \equiv 1 \pmod 8 \\ S_{(2)}, & \text{if } d \equiv 5 \pmod 8; \end{cases}$$

$$H_{2\varepsilon} \cap S_{(1)} = \{(1), (\sqrt{-d})\}S_{(4)};$$

$$H \cap S_{(1)} = \begin{cases} \{(1), (5), (\sqrt{-d}), (5\sqrt{-d})\}S_{(8)}, & 2 \mid \beta \\ \{(1), (5), (4+\sqrt{-d}), (4+5\sqrt{-d})\}S_{(8)}, & 2 \nmid \beta. \end{cases}$$

(2) $2 \mid d$*:*

$$H_{-1} \cap S_{(1)} = S_{(2)};$$

$$H_\varepsilon \cap S_{(1)} = H_{2\varepsilon} \cap S_{(1)} = S_{(4)};$$

$$H \cap S_{(1)} = \{(1), (5)\}S_{(8)}.$$

Proof We prove the case $d \equiv 1 \pmod 4$ for the ideal groups corresponding to $\mathbb{Q}(\sqrt[4]{2\varepsilon}, i)/\mathbb{Q}(\sqrt{-d})$ and its subextensions; the other assertions are proved in a similar way.

(1) Since $\mathbb{Q}(\sqrt{d}, i)/\mathbb{Q}(\sqrt{-d})$ is unramified, we have

$$H_{-1} \cap S_{(1)} = A_{(2)} \cap S_{(1)}.$$

(2) It is not hard to show (for instance by the conductor-discriminant formula, see [5, p. 136]) that the conductor of the abelian extension $\mathbb{Q}(\sqrt{2\varepsilon}, i)/\mathbb{Q}(\sqrt{-d})$ divides (4); hence $S_{(4)} \subseteq H_{2\varepsilon}$. As $\mathbb{Q}(\sqrt{2\varepsilon}, i)/\mathbb{Q}(\sqrt{-d})$ is ramified, we have $H_{2\varepsilon} \cap S_{(1)} \neq A_{(2)} \cap S_{(1)}$. We infer that

$$[A_{(2)} \cap S_{(1)} : H_{2\varepsilon} \cap S_{(1)}] = [H_{-1} \cap S_{(1)} : H_{2\varepsilon} \cap S_{(1)}] = 2.$$

Since $(\sqrt{-d}) \in H_{2\varepsilon} \cap S_{(1)}$ (by Proposition 2), we conclude that

$$H_{2\varepsilon} \cap S_{(1)} = \{(1), (\sqrt{-d})\} S_{(4)}.$$

(3) It is not difficult to show (for instance by the conductor-discriminant formula) that the conductor of the extension $\mathbb{Q}(\sqrt[4]{2\varepsilon}, i)/\mathbb{Q}(\sqrt{-d})$ divides (8); hence $S_{(8)} \subseteq H$. Using the fact that $A_{(2)}/H$ is cyclic one finds that $\left[\{(1), (\sqrt{-d})\} S_{(4)} : H \cap S_{(1)}\right] = 2$. As $A_{(2)} \cap S_{(1)}/S_{(4)}$ is not cyclic, we get $H \cap S_{(1)} \neq S_{(4)}$. From $(5) \in H$ (by Lemma 3) and $\{(1), (\sqrt{-d})\} S_{(4)} \supseteq H \cap S_{(1)} \supseteq S_{(8)}$ it follows that

$$H \cap S_{(1)} = \{(1), (5), (\sqrt{-d}), (5\sqrt{-d})\} S_{(8)}$$

or

$$H \cap S_{(1)} = \{(1), (5), (4 + \sqrt{-d}), (4 + 5\sqrt{-d})\} S_{(8)}.$$

Since

$$H \cap S_{(1)} = \{(1), (5), (\sqrt{-d}), (5\sqrt{-d})\} S_{(8)} \iff (\sqrt{-d}) \in H \cap S_{(1)} \iff 2|\beta$$

(*cf.* Proposition 2), we have proved what was asserted about $H \cap S_{(1)}$. ∎

We now turn to the proofs of the results of the previous section. We concentrate on $d \equiv 5 \pmod 8$; the other cases are similar .

The existence of a relation $p^{m_0} = d_1 s^2 + d_2 v^2$ follows by genus theory and if m_0 is minimal, it is not difficult to show that $m_0 | m$ and that if we write $d_1 = p_1^{a_1} \cdots p_{r-1}^{a_{r-1}}$, $a_1, \dots, a_{r-1} \in \{0, 1\}$, then, for a suitable sign of v, we have (where P_i is the prime ideal in $\mathbb{Q}(\sqrt{-d})$ above p_i)

$$\mathfrak{p}^{m_0} P_1^{a_1} \cdots P_{r-1}^{a_{r-1}} = (d_1 s + v\sqrt{-d}).$$

Note that

$$\Sigma_1 = \sum_{p_i \text{ of type II}} a_i.$$

Put

$$\Sigma_a := \sum_{p_i \equiv 5 \pmod 8} a_i.$$

One checks that

$$v \equiv \Sigma_a \pmod 2 \iff \big(4 | sv \wedge p \equiv 1 \pmod 8\big) \vee \big(4 \nmid sv \wedge p \equiv 5 \pmod 8\big).$$

https://doi.org/10.4153/CMB-2003-004-1 Published online by Cambridge University Press

We find that

$$\begin{aligned}
\mathfrak{p} \in H_\varepsilon &\iff \mathfrak{p}^{m_0} \in H_\varepsilon \\
&\iff \mathfrak{p}^{m_0} \cdot \prod_{P_i \equiv 5 \pmod 8} \big(P_i(\sqrt{-d})\big)^{a_i} \cdot \prod_{P_i \equiv 1 \pmod 8} P_i^{a_i} \in H_\varepsilon \\
&\iff \big(2|\Sigma_a \wedge (d_1 s + v\sqrt{-d}) \in H_\varepsilon\big) \\
&\qquad \vee \big(2 \nmid \Sigma_a \wedge (d_1 s + v\sqrt{-d})(\sqrt{-d}) \in H_\varepsilon\big) \\
&\iff (2|\Sigma_a \wedge 2|v) \vee (2 \nmid \Sigma_a \wedge 2 \nmid v) \\
&\iff v \equiv \Sigma_a \pmod 2 \\
&\iff \big(4|sv \wedge p \equiv 1 \pmod 8\big) \vee \big(4 \nmid sv \wedge p \equiv 5 \pmod 8\big)
\end{aligned}$$

and

$$\begin{aligned}
\mathfrak{p} \in H &\iff \mathfrak{p}^{m_0} \in H \\
&\iff \mathfrak{p}^{m_0} \cdot \prod_{P_i \text{ of type I}} P_i^{a_i} \cdot \prod_{P_i \text{ of type II}} \big(P_i(1+4\sqrt{-d})\big)^{a_i} \in H \\
&\iff \big(2|\Sigma_1 \wedge (d_1 s + v\sqrt{-d}) \in H\big) \\
&\qquad \vee \big(2 \nmid \Sigma_1 \wedge (d_1 s + v\sqrt{-d})(1+4\sqrt{-d}) \in H\big) \\
&\iff \begin{cases} (2|\Sigma_1 \wedge 8|sv) \vee (2 \nmid \Sigma_1 \wedge 4 \parallel sv), & 2|\beta \\ \big(2|\Sigma_1 \wedge (4 \parallel s \vee 8|v)\big) \vee \big(2 \nmid \Sigma_1 \wedge (8|s \vee 4 \parallel v)\big), & 2 \nmid \beta. \end{cases}
\end{aligned}$$

Note that $(\frac{\varepsilon_d}{p}) = 1$ if and only if $\mathfrak{p} \in H_\varepsilon$ and that $(\frac{\varepsilon_d}{p})_4 = 1$ if and only if $\mathfrak{p} \in H_\varepsilon \wedge \big((2|b \wedge \mathfrak{p} \in H) \vee (2 \nmid b \wedge \mathfrak{p} \notin H)\big)$, *cf.* Observation 1 and the observations at the beginning of this section. From this it is routine to deduce the criteria in the previous section. Note that $(\frac{2}{p})_4 = 1$ is equivalent to $2|b$ (if $p = a^2 + 16b^2$), *cf.* Remark 1.

5 A Similar Result

We state a general result for d even. It can be proved in a manner similar to the proofs in the previous section.

Theorem 13 *Let $d > 1$ be a square-free even integer, and assume that $N(\varepsilon_d) = -1$ (i.e., $x^2 - dy^2 = -1$ is solvable). Let $p \equiv 1 \pmod 4$ be a prime number such that $(\frac{d}{p}) = 1$. Let the class number of $\mathbb{Q}(\sqrt{-d})$ be $h\big(\mathbb{Q}(\sqrt{-d})\big) = 2^z m$, $2 \nmid m$. For $p \equiv 1 \pmod 8$ we write $p = a^2 + 16b^2$, $a, b \in \mathbb{Z}$. There are integers $g_1, \dots, g_r \in \mathbb{N}$ and prime numbers $\hat{p}_1, \dots, \hat{p}_r, \hat{q}_1, \dots, \hat{q}_r$ (depending only on d) such that the following statements hold:*

(1) *Let $p \neq \hat{p}_1, \dots, \hat{p}_r$. There is a minimal odd $m_0 \in \mathbb{N}$ such that*

https://doi.org/10.4153/CMB-2003-004-1 Published online by Cambridge University Press

$$p^{m_0}\hat{p}_1^{a_1}\cdots\hat{p}_r^{a_r}=s^2+dv^2$$

for suitable $a_i\in\{0,1,\dots,g_i\}$*;* $s,v\in\mathbb{Z}\setminus\{0\}$*. This minimal odd* m_0 *satisfies* $m_0\le m$*.*

(2) *Let* $p\neq\hat{q}_1,\dots,\hat{q}_r$*. There is a minimal odd* $m_0'\in\mathbb{N}$ *such that*

$$p^{m_0'}\hat{q}_1^{a_1'}\cdots\hat{q}_r^{a_r'}=(s')^2+d(v')^2$$

for suitable $a_i'\in\{0,1,\dots,g_i'\}$*;* $s',v'\in\mathbb{Z}\setminus\{0\}$*. This minimal odd* m_0' *satisfies* $m_0'\le m$*.*

(3) $\hat{q}_1,\dots,\hat{q}_r\neq p$*:*

$$\left(\frac{\varepsilon_d}{p}\right)=1\quad\Longleftrightarrow\quad 4|v'.$$

(4) $\hat{p}_1,\dots,\hat{p}_r,\hat{q}_1,\dots,\hat{q}_r\neq p\equiv 1\pmod 8$*:*

$$\left(\frac{\varepsilon_d}{p}\right)_4=1\quad\Longleftrightarrow\quad 4|v'\wedge\big((2|b\vee 8|v)\vee(2\nmid b\vee 8\nmid v)\big).$$

Theorem 14 *Let the assumptions and the notation be as in Theorem 13. Then*

(A) $\hat{q}_1,\dots,\hat{q}_r\neq p\equiv 5\pmod 8$*:*

$$x^2-dp^2y^2=-1\text{ is solvable}\iff 4\nmid v'.$$

(B) $\hat{p}_1,\dots,\hat{p}_r,\hat{q}_1,\dots,\hat{q}_r\neq p\equiv 9\pmod{16}$*:*

$$x^2-dp^2y^2=-1\text{ is solvable}\iff 4|v'\wedge\big((2\nmid b\vee 8|v)\vee(2|b\vee 8\nmid v)\big).$$

(C) $\hat{p}_1,\dots,\hat{p}_r,\hat{q}_1,\dots,\hat{q}_r\neq p\equiv 1\pmod{16}$*:*

$$x^2-dp^2y^2=-1\text{ is solvable}\implies 4|v'\wedge\big((2|b\vee 8|v)\vee(2\nmid b\vee 8\nmid v)\big).$$

Remark 4 If we choose prime ideals $\mathfrak{p}_1,\dots,\mathfrak{p}_r\in H$ and $\mathfrak{q}_1,\dots,\mathfrak{q}_r\in H_\varepsilon$ such that

$$\mathfrak{p}_1(A_{(2)}\cap S_{(1)}),\dots,\mathfrak{p}_r(A_{(2)}\cap S_{(1)})\quad\text{and}\quad\mathfrak{q}_1(A_{(2)}\cap S_{(1)}),\dots,\mathfrak{q}_r(A_{(2)}\cap S_{(1)})$$

are bases for the 2-Sylow group of $A_{(2)}/(A_{(2)}\cap S_{(1)})$ (where the ideal groups are as before), then $\hat{p}_1,\dots,\hat{p}_r,\hat{q}_1,\dots,\hat{q}_r$ can be taken as the norms of these prime ideals; put $g_i:=\operatorname{ord}\big(\mathfrak{p}_i(A_{(2)}\cap S_{(1)})\big)-1$ and $g_i':=\operatorname{ord}\big(\mathfrak{q}_i(A_{(2)}\cap S_{(1)})\big)-1$.

Example 4 We give an explicit criterion for $d=2\cdot 41$. This d with *arbitrary* p is not covered by the criteria in the previous sections since the class group of $\mathbb{Q}(\sqrt{-82})$ is isomorphic to $\mathbb{Z}/4$. We have $\varepsilon_{82}=9+\sqrt{82}$ of norm -1. Let $\mathfrak{p}_{13}$, $\mathfrak{p}_{29}$ be prime ideals in $\mathbb{Q}(\sqrt{-82})$ above 13, 29, respectively. Let $\bar{\mathfrak{p}}_{13}$, $\bar{\mathfrak{p}}_{29}$ be prime ideals in $\mathbb{Q}(\sqrt{82})$ above 13, 29, respectively. It is easily seen that each of

$$\mathfrak{p}_{13}(A_{(2)}\cap S_{(1)}),\quad\mathfrak{p}_{29}(A_{(2)}\cap S_{(1)})$$

https://doi.org/10.4153/CMB-2003-004-1 Published online by Cambridge University Press

generates $A_{(2)}/(A_{(2)} \cap S_{(1)})$ (with notation as before). Since

$$(2\varepsilon)^{\frac{N(\tilde{\mathfrak{p}}_{13})-1}{4}} = 2^3 \cdot (9+\sqrt{82})^3 \equiv 1 \pmod{13},$$

it follows that $\mathfrak{p}_{13} \in H$. Similarly, $\mathfrak{p}_{29} \in H_\varepsilon$. Hence we have the following criterion:

Let $p = a^2 + 16b^2 \equiv 9 \pmod{16}$ be a prime number with $(\frac{82}{p}) = 1$; write

$$p \cdot 13^{a_1} = s^2 + 82v^2, \quad p \cdot 29^{a_1'} = (s')^2 + 82(v')^2$$

where $a_1, a_1' \in \{0,1,2,3\}$ and $s, v, s', v' \in \mathbb{Z} \setminus \{0\}$. Then (since necessarily $p \neq 13, 29$)

$$x^2 - 82p^2y^2 = -1 \text{ is solvable } \iff 4|v' \wedge \big((2 \nmid b \vee 8|v) \vee (2|b \vee 8 \nmid v)\big).$$

References

[1] J. W. S. Cassels and A. Fröhlich, *Algebraic Number Theory.* Thompson, Washington D.C, 1967.

[2] P. G. L. Dirichlet, *Einige neue Sätze über unbestimmte Gleichungen.* Gesammelte Werke, Chelsea, New York, 219–236.

[3] Y. Furuta, *Norm of Units of Quadratic Fields.* J. Math. Soc. Japan **11**(1959), 139–145.

[4] F. Halter-Koch, *Konstruktion von Klassenkörpern und Potenzrestkriterien für quadratische Einheiten.* Manuscripta Math **54**(1986), 453–492.

[5] H. Hasse, *Vorlesungen über Klassenkörpertheorie.* Physica-Verlag, Würzburg, 1967.

[6] E. Hecke, *Lectures on the Theory of Algebraic Numbers.* Springer-Verlag, 1981.

[7] Chr. U. Jensen, *On the Solvability of a Certain Class of non-Pellian Equations.* Math. Scand. **10**(1962), 71–84.

[8] ———, *On the Diophantine Equation* $\xi^2 - 2m^2\eta^2 = -1$. Math. Scand. **11**(1962), 58–62.

[9] J. Perrot, *Sur l'equation* $t^2 - Dy^2 = -1$. J. Reine Angew. Math. **102**(1888), 185–223.

[10] L. Rédei, *Bedingtes Artinsymbol mit Anwendungen in der Klassenkörpertheorie.* Acta Math. Sci. Hung. **4**(1953), 1–29.

[11] ———, *Die 2-Ringklassengruppe des quadratischen Zahlkörpers und die Theorie der Pellschen Gleichung.* Acta Math. Sci. Hung. **4**(1953), 31–87.

[12] L. Rédei and H. Reichardt, *Die Anzahl der durch 4 teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörbers.* J. Reine Angew. Math. **170**(1934), 69–74.

[13] A. Scholz, *Über die Lösbarkeit der Gleichung* $t^2 - Du^2 = -4$. Math. Zeitschrift **39**(1935), 95–111.

Department of Mathematics
University of Copenhagen
DK-2100 Copenhagen
Denmark
email: tommy@math.ku.dk