JOURNAL OF NUMBER THEORY 43, 1–19 (1993)

Divisibility by 2-Powers of Certain Quadratic Class Numbers

PETER STEVENHAGEN

Faculteit Wiskunde en Informatica, Universiteit van Amsterdam, Plantage Muidergracht 24, 1018 TV Amsterdam, The Netherlands and CNRS-URA 741, 16, Route de Gray, 25030 Besançon Cedex, France

Communicated by M. Pohst

Received March 4, 1991; revised July 22, 1991

We study the divisibility of the strict class numbers of the quadratic fields of discriminant $8p$, $-8p$, and $-4p$ by powers of 2 for $p \equiv 1 \bmod 4$ a prime number. Various criteria for divisibility by 8 are discussed, and an analogue of the relation $8 \mid h_{8p}^{+} \Leftrightarrow 8 \mid h_{-8p}$ and $8 \mid h_{-4p}$ is given for divisibility by 16. We present numerical data related to the known and conjectured densities of primes p giving rise to specific 2-power divisibilities.

1. INTRODUCTION

Let $p \equiv 1 \bmod 4$ be a prime number. This paper discusses 2-power divisibilities of the (strict) class numbers of the three quadratic fields of discriminant $8p$, $-8p$, and $-4p$ and the relations between them. We will denote the ordinary class number of a quadratic field of discriminant f by h_f and its strict class number by h_f^+. If $f > 0$ we let ε_f be the fundamental unit of $\mathbb{Q}(\sqrt{f})$, so $h_f^+ = h_f$ unless we have $f > 0$ and $\mathrm{Norm}(\varepsilon_f) = 1$. In the latter case one has $h_f^+ = 2h_f$.

By genus theory, the 2-primary parts of the strict class groups of discriminants $f = 8p$, $-8p$, and $-4p$ are non-trivial cyclic 2-groups, so we know their complete structure when we know the highest power of 2 dividing the corresponding strict class numbers. In each of the three cases, it follows from a criterion of Rédei that these class numbers are divisible by 4 if and only if $p \equiv 1 \bmod 8$. This condition amounts to saying that p splits completely in the cyclotomic field $\mathbb{Q}(\zeta_8)$ obtained by adjoining a primitive 8th root of unity to $\mathbb{Q}$. In particular, we know that the set of primes satisfying this condition has natural density $\frac{1}{4}$.

In the literature [10, 14, 15, 16, 20, 22, 25], one encounters various conditions on p that ensure divisibility of the three class numbers by 8. The

0022-314X/93 $5.00

following are particularly relevant for our purposes, and we will furnish a short proof in Section 2.

THEOREM 1. *Let $p \equiv 1 \bmod 8$ be a prime number, and χ the quadratic character of conductor p. Let ζ_8 be an element of order 8 in $(\mathbb{Z}/p\mathbb{Z})^*$. Then we have*

$$8 \mid h_{4p} \Leftrightarrow \chi(1+\zeta_8^2) = 1;$$
$$8 \mid h_{8p} \Leftrightarrow \chi(1+\zeta_8^2)\,\chi(\zeta_8) = 1;$$
$$8 \mid h_{8p}^+ \Leftrightarrow \chi(1+\zeta_8^2) = \chi(\zeta_8) = 1.$$

This theorem shows that the divisibility of the class numbers by 8 is determined by the splitting behaviour of p in a *governing field* M. As $\zeta_8^2 = i$ and $\zeta_8 + \zeta_8^3 = \sqrt{-2}$, one can take M in the three cases of the theorem respectively equal to $\mathbb{Q}(\zeta_8, \sqrt{1+i})$, $\mathbb{Q}(\zeta_8, \sqrt[4]{-2})$, and $\mathbb{Q}(\zeta_8, \sqrt{1+i}, \sqrt[4]{-2}) = \mathbb{Q}(\zeta_{16}, \sqrt[4]{2})$.

It has been shown in [25] that the 8-rank of the class group of *any* quadratic order of discriminant Dp, for $D \not\equiv 2 \bmod 4$ an integer and p a variable prime, is determined by the splitting behaviour of p in a certain normal extension $M/\mathbb{Q}$. The corresponding statement for 2^k-ranks is not known to hold for a single value of D when $k > 3$. Apart from an observed density pattern for $D = -4$ and $D = 8$, there is only negative evidence, cf. [6]. As we will see, the problem stems from the fact that one does not know how to construct governing fields for the 2-adic behaviour of fundamental units like ε_p or ε_{8p} that occur in related quadratic fields. These units are naturally related to the class numbers we are interested in: first there are direct relations coming from analytic class number formulas over either the complex numbers [10, 18, 26] or $\mathbb{Q}_2$, and secondly there are the general continuity results of Gras for the 2-adic L-functions that yield class number congruences involving these units [9]. For instance, one has the following conditions of Williams [26] for the divisibility of h_{4p} by 8 and 16 in terms of the 2-adic logarithm of the fundamental unit ε_p. They are special cases of the analytic congruences we mentioned but we will see how to derive them algebraically in Section 2.

THEOREM 2. *Let $p \equiv 1 \bmod 8$ be a prime number and $\log_2 : \mathbb{Q}_2^* \to \mathbb{Q}_2$ the 2-adic logarithm. Then we have*

$$8 \mid h_{4p} \Leftrightarrow \log_2(\varepsilon_p) \equiv 0 \pmod 8;$$

$$16 \mid h_{4p} \Leftrightarrow \log_2(p\varepsilon_p) \equiv 0 \pmod{16}.$$

Even though there may not be a direct generalization of Theorem 1 for divisibility by 16, there is a weaker form

$$8 \mid h_{8p}^{+} \Leftrightarrow 8 \mid h_{\ 8p} \qquad \text{and} \qquad 8 \mid h_{\ 4p}. \tag{1}$$

which is due to Kaplan [15] that admits the following generalization.

THEOREM 3. *Let χ and ζ_8 be as in Theorem* 1, *and suppose* $\chi(1+\zeta_8^2) = \chi(\zeta_8) = 1$. *Then one has*

$$16 \mid h_{8p}^{+} \Leftrightarrow 16 \mid h_{\ 8p} \qquad \textit{and} \qquad 16 \mid h_{\ 4p}$$

for the primes p that satisfy $\chi(1+\zeta_8) = 1$, *and*

$$16 \mid h_{8p}^{+} \Leftrightarrow 16 \mid h_{\ 8p} \qquad \textit{and} \qquad 8 \parallel h_{\ 4p}.$$

for the primes p that satisfy $\chi(1+\zeta_8) = -1$.

The implication $16 \mid h_{8p} \Rightarrow 16 \mid h_{\ 8p}$ that follows from this theorem had already been obtained by Oriat [23] by a careful application of reflection principles in the field $\mathbb{Q}(\zeta_8, \sqrt{p})$. Our proof of Theorem 3 will be essentially analytic, based on a method of Bucher. The relevance of Bucher's result in the present context was noted by Buell, Kaplan, and Williams [4, 19], and Theorem 3 can be seen as a sharpening of the main result in [19]. The original paper of Bucher [3] is somewhat obscure in the sense that it appeared in an unknown Swiss journal and was missed by the Zentralblatt because of the war. Moreover its main argument—a norm computation in a cyclotomic field—can be given much more efficiently when one does without Bucher's numerous trigonometric formulas and introduces a simple ramification argument. We will do this in Section 3.

The final section compares the empirical density behaviour of primes giving rise to certain types of 2-class groups with the density that would follow from reasonable but unproved assumptions on the 2-adic behaviour of units.

2. CONDITIONS FOR 2-POWER DIVISIBILITY

This section contains the proofs of all theorems stated in the introduction and discusses several other conditions for 2-power divisibility of the three class numbers we consider. We need some generalities before we can begin the actual proofs.

Let $\mathcal{C}(f)$ and $H(f)$ denote respectively the strict class group and the strict Hilbert class field of the quadratic field of discriminant f. The extension $H(f)/\mathbb{Q}(\sqrt{f})$ is Galois with group (canonically isomorphic to)

$\mathcal{C}(f)$, so we may define for each 2-power $t = 2^k$ the t-Hilbert class field $H_t = H_t(f)$ of $\mathbb{Q}(\sqrt{f})$ as the subfield of $H(f)$ that is fixed by $\mathcal{C}(f)^t$. The group $G = \mathrm{Gal}(H(f)/\mathbb{Q}(\sqrt{f}))$ is generalized dihedral: it is the semi-direct product of $\mathcal{C}(f)$ with a group of order two whose generator acts on $\mathcal{C}(f)$ as -1. The field H_2 left invariant by the commutator subgroup $[G, G] = \mathcal{C}(f)^2$ of G is the genus field of $\mathbb{Q}(\sqrt{f})$. It can be given explicitly for any f, and for $f = 8p$, $-8p$, or $-4p$ with $p \equiv 1 \bmod 4$ prime it is obtained by adjoining $\sqrt{p}$ to $\mathbb{Q}(\sqrt{f})$. In each of these three cases the quadratic subfield $K = \mathbb{Q}(\sqrt{fp})$ of $H_2(f)$ does not depend on p; it has discriminant respectively 8, -8, and -4.

Proof of Theorem 1. We consider the extension $H_4 = H_4(f)$ of K for $f \in \{\pm 8p, -4p\}$, with K defined as above. This is a normal extension of degree 2 or 4 that is unramified at all finite primes outside p and has ramification index 2 at the primes over p. By looking at the ramification group of a prime over p, one sees that $\mathrm{Gal}(H_4/K)$ is abelian and of exponent 2. Conversely, let N be the maximal abelian extension of K that is unramified at all finite primes outside p and of exponent 2. Obviously N contains $H_2(f)$. As K has strict class number $h_K^+ = 1$, the inertia groups at the primes over p generate $\mathrm{Gal}(N/K)$, so $[N : K] \leqslant 4$. Further N is unramified and normal over $\mathbb{Q}(\sqrt{f})$ as it is unramified over $H_2(f)$ and normal over $\mathbb{Q}$. We conclude that $N = H_4$, so $4 \mid h_f^+$ if and only if $[N : K] = 4$.

In case we have $4 \mid h_f^+$, we can decide whether $8 \mid h_f^+$ by looking at the image of the unique element of order 2 in $\mathcal{C}(f)$ in the factor group $\mathcal{C}(f)/\mathcal{C}(f)^4$ corresponding to $\mathrm{Gal}(H_4/\mathbb{Q}(\sqrt{f}))$. One has divisibility by 8 exactly when this element is in the kernel, i.e., when a prime of $\mathbb{Q}(\sqrt{f})$ lying in this class splits completely in H_4. For $f = -4p$ or $f = -8p$ the unique prime over 2 in $\mathbb{Q}(\sqrt{f})$ is obviously not principal, so its ideal class generates the 2-torsion of $\mathcal{C}(f)$. Note that the prime over p is also in this ideal class. For $f = 8p$ this need not be true, but one knows that the 2-torsion of $\mathcal{C}(f)$ is generated by the classes of the primes over 2 and p. The product of these classes is the ideal class of $(\sqrt{8p})$, which has trivial image in $\mathcal{C}(8p)/\mathcal{C}(8p)^4$ if and only if the corresponding field H_4 is real.

We can describe the Galois group $\mathrm{Gal}(H_4/K)$ by class field theory. In the easier cases $f = -4p$ and $f = -8p$, which we will deal with first, it is simply the ray class group $\mathcal{R}_p$ of conductor p modulo its squares. Writing $\mathcal{O}_K$ for the ring of integers of K, one has $\mathcal{R}_p = (\mathcal{O}_K/p\mathcal{O}_K)^*/\mathrm{im}(\mathcal{O}_K^*)$.

For $f = -4p$ the prime p splits in $K = \mathbb{Q}(i)$ and one sees that $\mathcal{R}_p/\mathcal{R}_p^2$ has order 4 if and only if the generator i of $\mathcal{O}_K^*$ is a square modulo the primes over p, i.e., if and only if $p \equiv 1 \bmod 8$. If this is the case, one has $8 \mid h_{4p}$ exactly when the prime over 2 splits completely in $H_4/\mathbb{Q}(\sqrt{-4p})$. Looking

at the extension H_4/K instead, one sees that this happens precisely when the Frobenius of the prime $(1+i)$ is the trivial element in $\mathscr{R}_p/\mathscr{R}_p^2$. One finds that $8 \mid h_{4p}$ if and only if $1+i$ is a square modulo the primes in K over p, i.e., when $\chi(1+\zeta_8^2)=1$.

For $f=-8p$ one has $K=\mathbb{Q}(\sqrt{-2})$ and the group $\mathscr{R}_p/\mathscr{R}_p^2$ has order 4 if and only if the prime $p \equiv 1 \bmod 4$ splits in $K/\mathbb{Q}$, i.e., if and only if $p \equiv 1 \bmod 8$. If this is the case, one has $8 \mid h_{8p}$ exactly when the prime $(\sqrt{-2})$ splits completely in H_4/K. One finds that $8 \mid h_{8p}$ if and only if $\sqrt{-2}$ is a square modulo the primes in K over p, i.e., when $\chi(\zeta_8+\zeta_8^3)=1$.

Finally, let $f=8p$, so $K=\mathbb{Q}(\sqrt{2})$ is real. We now describe $\mathrm{Gal}(H_4/K)$ as the ray class group $\mathscr{R}_{p\cdot\infty}$ of conductor $p\cdot\infty$ modulo its squares, with ∞ the product of the two real primes of K. One has

$$\mathscr{R}_{p\cdot\infty} = [(\mathscr{O}_K/p\mathscr{O}_K)^* \times \langle -1 \rangle \times \langle -1 \rangle]/\mathrm{im}(\mathscr{O}_K^*),$$

with $\mathscr{O}_K^*$ mapping naturally to the first factor and via the sign maps at the real primes to the groups $\langle -1 \rangle$. As the fundamental unit $\varepsilon_2 = 1+\sqrt{2}$ of K has norm -1, the unit group $\mathscr{O}_K^*$ maps surjectively to $\langle -1 \rangle \times \langle -1 \rangle$ and $\mathscr{R}_{p\cdot\infty}/\mathscr{R}_{p\cdot\infty}^2$ has order 4 if and only if $p \equiv 1 \bmod 4$ splits completely in $K/\mathbb{Q}$. We conclude that $4 \mid h_{8p}^+$ if and only if $p \equiv 1 \bmod 8$. Assuming this, we have $8 \mid h_{8p}^+$ if and only if the classes of primes over 2 and p generate the trivial subgroup in $\mathscr{C}(8p)/\mathscr{C}(8p)^4$, i.e., if and only if $(\sqrt{2})$ splits completely in H_4/K and H_4 is real. This comes down to requiring that $\mathscr{R}_p/\mathscr{R}_p^2$ already has order 4 and that $\sqrt{2}$ has trivial image in this group. This means that $\sqrt{2}$ and $1+\sqrt{2}$ are squares modulo the primes in K over p or, equivalently, that $\chi(\zeta_8+\zeta_8^{-1})=1=\chi(1+\zeta_8+\zeta_8^{-1})$. We have obtained the conditions of Theorem 1 because $\chi(\zeta_8+\zeta_8^{-1})=\chi(\zeta_8)\,\chi(1+\zeta_8^2)$ and $\chi(1+\zeta_8+\zeta_8^{-1})\,\chi(1+\zeta_8^2) = \chi(1+\zeta_8)^2=1$. This finishes the proof of Theorem 1. ∎

There exist many other criteria for the divisibility by 8 of the class numbers in Theorem 1, and most of them can be derived by arguments similar to those given above. We will briefly discuss a few conditions to show this.

If one assume $p \equiv 1 \bmod 8$, there exists in all three cases we are dealing with a prime element $\pi \mid p$ in $\mathscr{O}_K$, uniquely determined up to multiplication by squares in $\mathscr{O}_K^*$ and conjugation in K, such that $H_4=K(\sqrt{\pi},\sqrt{\bar{\pi}})$. The splitting behaviour of the primes over 2, p, and ∞ in $H_4/\mathbb{Q}(\sqrt{f})$ can easily be expressed in terms of π.

The prime over 2 splits completely in $H_4/\mathbb{Q}(\sqrt{f})$ if and only if the prime $\mathfrak{a} \mid 2$ in K splits completely in H_4/K. This happens when π is a square in the completion of K at $\mathfrak{a}$, i.e., when $\pi \bmod \mathfrak{a}^5$ is congruent to ± 1 when $f=-4p$, to 1 or $-1+2\sqrt{-2}$ when $f=-8p$ and to 1 or $3+2\sqrt{2}$ when $f=8p$. The prime over p splits completely in $H_4/\mathbb{Q}(\sqrt{f})$ when π is a square mod $\bar{\pi}$, i.e, when the Legendre symbol $(\pi/\bar{\pi})=(\mathrm{Tr}(\pi)/p)$ equals 1. Finally, if $f=8p$, the field H_4 is real when π is totally positive.

Thus, writing $\pi\varepsilon$ with $\varepsilon \in \mathcal{O}_K^*$ in the cases $f = -4p$, $-8p$, and $8p$ respectively as $a+bi$, $c+d\sqrt{-2}$ and $u+v\sqrt{2}$ with $a, c, u \equiv 1 \bmod 4$ and $u > 0$, one has representations

$$p = a^2 + b^2 = c^2 + 2d^2 = u^2 - 2v^2 \qquad (a, c, u \equiv 1 \bmod 4;\ u > 0) \qquad (2)$$

of the prime p that are unique up to the choice of the sign of b, d, and v and applications of the transformation $(u, v) \mapsto (17u + 24v,\ 12u + 17v)$ reflecting multiplication by $(1+\sqrt{2})^4$. In terms of these representations one obtains

$$8 \mid h_{4p} \Leftrightarrow (a, b) \equiv (1, 0) \text{ or } (5, 4) \bmod 8 \Leftrightarrow \left(\frac{a}{p}\right) = 1;$$

$$8 \mid h_{8p} \Leftrightarrow c \equiv 1 \bmod 8 \Leftrightarrow \left(\frac{c}{p}\right) = 1;$$

$$8 \mid h_{8p}^+ \Leftrightarrow u \equiv 1 \bmod 8 \text{ and } 4 \mid v \Leftrightarrow \left(\frac{u}{p}\right) = 1 \text{ and } 4 \mid v.$$

In each of the three cases the "middle condition" simply means that p splits completely in respectively the ray class field of $\mathbb{Q}(i)$ modulo $(1+i)^5$, the maximal subfield of the ray class field of $\mathbb{Q}(\sqrt{-2})$ modulo $\sqrt{-2}^5$ that is of exponent 2 over $\mathbb{Q}(\sqrt{-2})$, and the ray class field module $\sqrt{2}^5 \cdot \infty$ of $\mathbb{Q}(\sqrt{2})$. One easily checks that these three fields are indeed the governing fields $\mathbb{Q}(\zeta_8, \sqrt{1+i})$, $\mathbb{Q}(\zeta_8, \sqrt[4]{-2})$, and $\mathbb{Q}(\zeta_{16}, \sqrt[4]{2})$ from Theorem 1. The first two of these fields can also be viewed as the ring class fields modulo 4 and 8 of respectively $\mathbb{Q}(\sqrt{-2})$ and $\mathbb{Q}(i)$, so the primes that split completely in them are exactly those that are represented by the corresponding principal quadratic forms. One obtains the equivalences

$$8 \mid h_{4p} \Leftrightarrow p = x^2 + 32y^2$$
$$8 \mid h_{8p} \Leftrightarrow p = x^2 + 64y^2.$$

Note that we restrict here to $p \equiv 1 \bmod 4$. For primes $p \equiv -1 \bmod 4$ one can also have $8 \mid h_{8p}$, and by an argument analogous to the proof of Theorem 1 this happens if and only if $p \equiv -1 \bmod 16$. However, for such primes the orders of $\mathcal{C}(8p)$ and $\mathcal{C}(-4p)$ (a ring class group) are never divisible by 4, and this explains why we further disregard this case. If one chooses to work with the explicit "coordinates" u and v from (2), there is still another approach to the various 8-divisibilities. Rewriting the relation $p = u^2 - 2v^2$ as

$$(u + 2v)^2 + p = 2(u + v)^2 \qquad \text{and} \qquad 4v^2 + 2p = 2u^2,$$

one considers the principal ideals in $\mathbb{Q}(\sqrt{-p})$ and $\mathbb{Q}(\sqrt{-2p})$ that are generated by $u+2v+\sqrt{-p}$ and $2v+\sqrt{-2p}$. Obviously, these ideals are products of pairwise non-conjugate prime ideals of degree 1. From their norms, one sees that they factor as a product of the prime $\mathfrak{a}$ over 2 and the *square* of some ideal $\mathfrak{g}$ of norm respectively $u+v$ and u. The ideal $\mathfrak{g}$ is a square root of $\mathfrak{a}$ in the class group, so it is a 4-torsion element. One has divisibility of h_{4p} and h_{8p} by 8 if and only if in each case the ideal $\mathfrak{g}$ is a square, i.e., if and only if the Artin symbol of $\mathfrak{g}$ is trivial on the genus field H_2. The genus field $H_2 = H_2(f)$ can be obtained by adjoining $\sqrt{-1}$ or $\sqrt{p}$ to $\mathbb{Q}(\sqrt{f})$ in case $f=-4p$, and by adjoining $\sqrt{-2}$ or $\sqrt{p}$ in case $f=-8p$. The action of the Artin symbol of $\mathfrak{g}$ on these square roots $\sqrt{x}$ is simply the action of the Artin symbol of the norm of $\mathfrak{g}$ to $\mathbb{Q}$ in the extension $\mathbb{Q}(\sqrt{x})/\mathbb{Q}$, and one obtains the following conditions of Brown [2] and Hasse [11–13].

$$8 \mid h_{4p} \Leftrightarrow 4 \mid v \Leftrightarrow \left(\frac{u+v}{p}\right) = 1;$$

$$8 \mid h_{8p} \Leftrightarrow u \equiv 1 \bmod 8 \Leftrightarrow \left(\frac{u}{p}\right) = 1.$$

Note that together with the condition for $8 \mid h_{8p}^{+}$ above, these conditions give a different proof for Kaplan's equivalence (1). One can continue the idea of the proof above and extract a square root of the ideal class of $\mathfrak{g}$ to obtain 8-torsion ideal classes. This yields conditions for divisibility by 16 as given in [21] and [17]. They are different from the conditions obtained by looking 4- and 8-class fields [27], and none of these results leads to a construction of governing fields or density statements of any kind.

The conditions of the type given in Theorem 2 can be obtained by considering the 4-Hilbert class fields H_4 as extensions of $\mathbb{Q}(\sqrt{p})$. Assuming again $p \equiv 1 \bmod 8$, the extensions $H_4/\mathbb{Q}(\sqrt{p})$ are abelian of type 2×2 and of conductor dividing $8 \cdot \infty$. For $f=-4p$ the conductor even divides $4 \cdot \infty$ and H_4 can be obtained from $\mathbb{Q}(\sqrt{p})$ by adjunction of square roots of units, so one has $H_4 = \mathbb{Q}(i, \sqrt{p}, \sqrt{\varepsilon_p})$, with ε_p the fundamental unit of $\mathbb{Q}(\sqrt{p})$. Let $\tau \in \mathbb{Q}(\sqrt{p})$ be an element that generates an odd power of one of the primes in $\mathbb{Q}(\sqrt{p})$ over 2. Such an element exists because the class number of $\mathbb{Q}(\sqrt{p})$ is odd. Multiplying τ if necessary by a unit, one may assume that τ has positive norm and that under the embedding $\phi: \mathbb{Q}(\sqrt{p}) \rightarrowtail \mathbb{Q}_2$ corresponding to the other prime over 2 one has $\phi(\tau) \equiv 1 \bmod 4$. The 4-Hilbert class fields H_4 for $f=8p$ and $f=-8p$ are then given by $H_4 = \mathbb{Q}(\sqrt{2}, \sqrt{p}, \sqrt{\tau})$ and $H_4 = \mathbb{Q}(\sqrt{-2}, \sqrt{p}, \sqrt{\tau\varepsilon_p})$, where the fundamental unit ε_p is chosen to satisfy $\phi(\varepsilon_p) \equiv 1 \bmod 4$.

The fact that the 4-Hilbert class fields for $f=-4p$, $f=-8p$, and $f=8p$

are the normal closures of respectively $\mathbb{Q}(\sqrt{\varepsilon_p})$, $\mathbb{Q}(\sqrt{\tau\varepsilon_p})$, and $\mathbb{Q}(\sqrt{\tau})$ also shows that Kaplan's divisibility result (1) mentioned in the introduction is not so much a "curious result" [22] but has a "natural explanation" coming from the relation between the fields H_4. More precisely, if h_{4p} and h_{8p} are both divisible by 8, we see from the splitting behaviour of the primes over 2 and p in the corresponding fields H_4 that each of the fields $\mathbb{Q}(\sqrt{\varepsilon_p})$ and $\mathbb{Q}(\sqrt{\tau\varepsilon_p})$ can be embedded in both $\mathbb{Q}_2$ and $\mathbb{Q}_p$. The same is then obviously true for $\mathbb{Q}(\sqrt{\tau})$, and we obtain $8 \mid h_{8p}^+$ by the same argument. Conversely, if $8 \mid h_{8p}^+$ we know that $\mathbb{Q}(\sqrt{\tau})$ can be embedded in $\mathbb{Q}_2$, and the fact that it is totally real implies that it has conductor $\mathfrak{t}^3$ over $\mathbb{Q}(\sqrt{p})$, with $\mathfrak{t}$ the prime over 2 dividing τ. Looking as above at the explicit form of the ray class group modulo $\mathfrak{t}^3$, one sees that -1 and ε_p generate a group of order 2 modulo $\mathfrak{t}^3$. This implies that $\mathbb{Q}(\sqrt{\varepsilon_p})$ can be embedded in $\mathbb{Q}_2$, so the same is true for $\mathbb{Q}(\sqrt{\tau\varepsilon_p})$ and we obtain from the splitting of the prime over 2 in the fields H_4 that 8 divides both h_{4p} and h_{8p}.

Proof of Theorem 2. We have $8 \mid h_{4p}$ if and only if the prime over 2 in $\mathbb{Q}(\sqrt{-4p})$ splits completely in H_4, and as we already observed this happens if and only if the field $F = \mathbb{Q}(\sqrt{p}, \sqrt{\varepsilon_p})$ admits an embedding into $\mathbb{Q}_2$. This condition means that ε_p can be mapped to a square in $\mathbb{Q}_2$, which is equivalent to the requirement $\phi(\varepsilon_p) \equiv 1 \bmod 8$ or, more canonically, $\log_2 \varepsilon_p = 0 \bmod 8$. This proves the first equivalence of Theorem 2. We remark that the same argument for $f = -8p$ gives the equivalence $8 \mid h_{8p} \Leftrightarrow \log_2 \tau\varepsilon_p \equiv 0 \bmod 8$.

Assuming $8 \mid h_{4p}$, there is a similar argument for divisibility by 16 that is obtained by looking at the extension H_8/F, which is again abelian of type 2×2. The argument works in this special case because explicit generators of H_8 have been given by Cohn [5]. With our choices of τ and ε_p, one has $H_8 = H_2(\sqrt[4]{\tau^2\varepsilon_p})$. Indeed, we note that the right hand side is a normal extension of $\mathbb{Q}$ because the product of $\tau^2\varepsilon_p$ and its conjugate in $\mathbb{Q}(\sqrt{p})$ is a power of $-4 = (1+i)^4$, and that it is unramified over H_2 because $\phi(\tau^2\varepsilon_p) \equiv 1 \bmod 8$. The prime over 2 splits completely in H_8/H_2 if and only if the embedding $\phi: \mathbb{Q}(\sqrt{p}) \to \mathbb{Q}_2$ admits an extension to $\mathbb{Q}(\sqrt[4]{\tau^2\varepsilon_p})$, so we have $16 \mid h_{4p}$ if and only if $\log_2(\tau^2\varepsilon_p) \equiv 0 \bmod 16$. It remains to prove that $\log_2 \tau^2 \equiv \log_2 p \bmod 16$.

If $p \equiv 1 \bmod 16$, we have $\chi(\zeta_8) = 1$ and $8 \mid h_{4p} \Leftrightarrow 8 \mid h_{8p}$ in Theorem 1, so our assumption and the remark above show that $\log_2 \tau \equiv \log_2 \tau\varepsilon_p \equiv 0 \bmod 8$. It follows that indeed $\log_2 \tau^2 \equiv \log_2 p \equiv 0 \bmod 16$. If $p \equiv 9 \bmod 16$, we have $8 \nmid h_{8p}$ and consequently $\log_2 \tau^2 \equiv \log_2 p \equiv 8 \bmod 16$. This proves Theorem 2. ∎

Let ε_{8p} be the fundamental unit of $\mathbb{Q}(\sqrt{8p})$, and $\eta_{8p} \in \{\varepsilon_{8p}, \varepsilon_{8p}^2\}$ the smallest positive power of ε_{8p} that has norm $+1$. Assuming the hypothesis

$8 \mid h_{8p}^+$ from Theorem 3, we will decide whether 16 divides h_{8p}^+ by determining whether $\eta_{8p}^{h_{8p}^+ 8} = \varepsilon_{8p}^{h_{8p}^+ 4}$ is an even power of η_{8p} or not. This will be done using Bucher's evaluation of this expression modulo $\sqrt{8p}$. We first need $\eta_{8p} \bmod \sqrt{8p}$ itself. If we write $\eta_{8p} = u + v\sqrt{2p}$, then v is even as η_{8p} has norm $+1$, so we want to know $u \bmod 4$ and $u \bmod p$. It turns out that there are three possibilities, depending on the generators of the 2-torsion subgroup of $\mathcal{C}(8p)$. We saw already that this subgroup has order 2, and that it is generated by the classes of the primes lying over 2 and p. If ε_{8p} has norm -1, then these classes coincide and neither of the primes over 2 or p is principal. If ε_{8p} has norm $+1$, then either the prime over 2 or the prime over p is in the principal class in $\mathcal{C}(8p)$. In the first case 2 is an integral norm from $\mathbb{Q}(\sqrt{8p})$, and in the second case p and also -2 are. Thus, we distinguish the three cases by the value of E_{8p}, which is by definition the unique element in $\{-1, -2, 2\}$ that is an integral norm from $\mathbb{Q}(\sqrt{2p})$.

LEMMA. *Let $\eta_{8p} = u + v\sqrt{2p}$ with $u > 0$ and E_{8p} be as above. Then we have*

$$E_{8p} = -1 \Leftrightarrow u \equiv 3 \bmod 32, \qquad u \equiv -1 \bmod p \text{ and } 2 \parallel v;$$

$$E_{8p} = 2 \Leftrightarrow u \equiv 3 \bmod 32, \qquad u \equiv 1 \bmod p \text{ and } 2 \parallel v;$$

$$E_{8p} = -2 \Leftrightarrow u \equiv 1 \bmod 16, \qquad u \equiv -1 \bmod p \text{ and } 4 \mid v.$$

In particular, one has $\eta_{8p}^k \equiv 1 \bmod \sqrt{8p}$ for $k \in \mathbb{Z}$ if and only if k is even.

Proof. If $E_{8p} = -1$ we have $\varepsilon_{8p} = s + t\sqrt{2p}$ with $s^2 - 2pt^2 = -1$, which can only hold modulo 4 if both s and t are odd. It follows that $u = s^2 + 2pt^2 = 4pt^2 - 1$ and $v = 2st$ satisfy the stated congruences.

If $E_{8p} = 2$, there exists $\alpha = a + b\sqrt{2p}$ such that $N\alpha = a^2 - 2pb^2 = 2$. Obviously b is odd, $2 \parallel a$ and $a^2 \equiv 2 \bmod p$. The element $\alpha^2/2$ is a totally positive unit in $\mathbb{Z}[\sqrt{2p}]$, whence a power of ε_{8p}. Changing α by a power of ε_{8p}, we may assume that $\alpha^2/2$ equals 1 or ε_{8p}. As clearly $\alpha^2/2 \neq 1$, we have

$$\varepsilon_{8p} = \alpha^2/2 = (a^2 + 2pb^2 + 2ab\sqrt{2p})/2 = a^2 - 1 + ab\sqrt{2p}.$$

From $u = a^2 - 1$ and $v = ab$ the congruences are immediate.

For $E_{8p} = -2$ one applies the same argument with $a^2 - 2pb^2 = -2$ to obtain $\varepsilon_{8p} = a^2 + 1 + ab\sqrt{2p}$. As we now have b odd, $4 \mid a$ and $a^2 \equiv 2 \bmod p$, the congruence follows.

As in all cases either $u \equiv -1 \bmod 4$ or $u \equiv -1 \bmod p$, we have $\eta_{8p}^k \equiv 1 \bmod \sqrt{8p}$ if and only if k is even. ∎

We now invoke Bucher's result. As for the notation, the biquadratic residue symbol $(x/2)_4$ is the quadratic character on $1+8\mathbb{Z}_2$ with kernel $1+16\mathbb{Z}_2=(\mathbb{Z}_2^*)^4$, i.e.,

$$\left(\frac{x}{2}\right)_4=(-1)^{(1/8)\log_2 x}\equiv\frac{1+3x}{4}\bmod 4 \qquad \text{for} \quad x\in 1+8\mathbb{Z}_2.$$

THEOREM (Bucher). *Let p be as in Theorem 3 and define $\sigma=(-1)^l$ with l the number of quadratic residues in the interval $(0, p/8)$. Viewing $\varepsilon_p\sqrt{p}$ as an element in $1+4\mathbb{Z}_2$ and choosing η_{8p} totally positive, one has the congruences*

$$\eta_{8p}^{h_{8p}^+/8}=\varepsilon_{8p}^{h_{8p}/4}\equiv\sigma\left(\frac{\varepsilon_p\sqrt{p}}{2}\right)_4 \bmod(2\sqrt{2})$$

and

$$\eta_{8p}^{h_{8p}^+/8}=\varepsilon_{8p}^{h_{8p}/4}\equiv\sigma\left(\frac{\varepsilon_2\sqrt{2}}{p}\right)_4 \bmod(\sqrt{p}).$$

We will give a proof of this result in the next section.

Proof of Theorem 3. This simply comes down to an evaluation of the quantities in Bucher's theorem. We will show that

$$\sigma\left(\frac{\varepsilon_p\sqrt{p}}{2}\right)_4=(-1)^{h_{8p}/8}$$

and

$$\sigma\left(\frac{\varepsilon_2\sqrt{2}}{p}\right)_4=\chi(1+\zeta_8)(-1)^{h_{4p}/8}(-1)^{h_{8p}/8},$$

which immediately establishes Theorem 3 as h_{8p}^+ is divisible by 16 if and only if these quantities are both equal to 1. Thus, it suffices to prove the following lemma.

LEMMA. *Suppose p satisfies the conditions of Theorem 3 and ζ_{16} denotes an element of order 16 in $(\mathbb{Z}/p\mathbb{Z})^*$. Then one has*

$$\left(\frac{\varepsilon_p\sqrt{p}}{2}\right)_4=\chi(\zeta_{16})(-1)^{h_{4p}/8} \qquad \textit{and} \qquad \left(\frac{\varepsilon_2\sqrt{2}}{p}\right)_4=\chi(\zeta_{16})\,\chi(1+\zeta_8);$$

$$\sigma=\chi(\zeta_{16})(-1)^{h_{4p}/8}(-1)^{h_{8p}/8}.$$

Proof. One has $\frac{1}{8}\log_2(\varepsilon_p\sqrt{p})=\frac{1}{8}\log_2 p\varepsilon_p-\frac{1}{16}\log_2 p\equiv\frac{1}{8}h_{4p}+\frac{1}{16}\log_2 p \bmod 2$ by Theorem 2, and this yields the first identity as $\chi(\zeta_{16})=(-1)^{(1/16)\log_2 p}$. The second identity $(\varepsilon_2\sqrt{2}/p)_4=\chi(\zeta_{16}+\zeta_{16}^{-1})=\chi(\zeta_{16})\,\chi(1+\zeta_8)$ follows from the relation $(\zeta_{16}+\zeta_{16}^{-1})^2=2+\sqrt{2}=\varepsilon_2\sqrt{2}$.

It turns out that the number l in the definition of σ has already been determined by Gauss [8, Sect. IX] as being equal to $\frac{1}{8}((p-1)/2 + h_{4p} + h_{8p})$, which immediately gives the result. Gauss's formulas for the distribution of the quadratic residues modulo p over the "octants" of the interval $(0, p)$ are in a manuscript that remained unpublished during Gauss's lifetime, and no proof by Gauss himself exists. Dedekind shows in his commentary on the manuscript in the collected works of Gauss [8, p. 301] how one can use analytic class number formulas of Dirichlet to express the character sums $\sum_{a \in S} \chi(a)$ for any of the eight octants S of $(0, p)$ in terms of h_{4p} and h_{8p}. His approach generalizes to all odd squarefree p and gives Gauss's formula in the special case that p is prime. ∎

If we have $8 \| h_{8p}^+$, then $\eta_{8p}^{h_{8p}^+/8} = \varepsilon_{8p}^{h_{8p}/4} \equiv \eta_{8p} \bmod \sqrt{8p}$ and one can find the two expressions occurring in Bucher's theorem from the values of the number E_{8p}. One obtains the following.

THEOREM. *Let χ and ζ_8 be as above, and suppose $8 \| h_{8p}^+$. Then the values of h_{8p} and h_{4p} depend as follows on E_{8p} and $\delta = \chi(1+\zeta_8)$.*

E_{8p}	$h_{8p} \bmod 16$	$h_{4p} \bmod 16$ if $\delta = 1$	$h_{4p} \bmod 16$ if $\delta = -1$
-1	8	16	8
2	8	8	16
-2	16	8	16

3. BUCHER'S RESULT

In this section we will prove the theorem of Bucher used in the proof of Theorem 3. We only used Bucher's congruence for $\eta_{8p}^{h_{8p}^+/8}$, but the theorem holds identically for $\eta_{qp}^{h_{qp}^+/8}$, where $q \equiv 1 \bmod 4$ is any prime number such that $8 | h_{qp}^+$ and η_{qp} is the smallest positive power of ε_{qp} that has norm $+1$. In order to avoid problems with signs, we will further fix roots of unity $\zeta_n = e^{2\pi i/n}$ in the field of complex numbers. We write $\lambda_n = (1-\zeta_n)(1-\zeta_n^{-1})$. Note that for n prime, this is a prime element over n in the real cyclotopic subfield $\mathbb{Q}(\zeta_n)$. Square roots of positive real numbers are from now on positive, and fundamental units will always be chosen to be >1. In particular, the numbers η_{qp} are totally positive. Finally, we let $\sigma_{q,p} \in \{\pm 1\}$ be the sign of the real number $N_{\mathbb{Q}(\lambda_q, \lambda_p)/\mathbb{Q}(\lambda_q)}(\lambda_q - \lambda_p)$, where p and q are different and either $1 \bmod 4$ or equal to 8. Note that $\sigma_{p,q} = (-1)^{((p-1)/4)((q-1)/4)} \sigma_{q,p}$ when p and q are both prime, and that $\sigma_{8,p} = (-1)^{(p-1)/4} \sigma_{8,p}$ when p is prime.

With these conventions, the main results of [3] can be stated in the following unified form.

THEOREM 4. *Suppose $q = 8$ or $q \equiv 1 \bmod 4$ is prime, and let $p \equiv 1 \bmod 4$ be a prime different from q such that $8 \mid h_{qp}^{+}$. Reading $(\cdot/q)_4 = (\cdot/2)_4$ for $q = 8$, one has congruences*

$$\eta_{qp}^{h_{qp}^{+}/8} \equiv \sigma_{p,q}\left(\frac{\varepsilon_p\sqrt{p}}{q}\right)_4 \bmod(\sqrt{q}) \quad \text{and} \quad \eta_{qp}^{h_{qp}^{+}/8} h \equiv \sigma_{q,p}\left(\frac{\varepsilon_q\sqrt{q}}{p}\right)_4 \bmod(\sqrt{p}).$$

As $\sigma_{p,8} = \sigma_{8,p}$ is determined by the parity of the number of conjugates of $\lambda_8 - \lambda_p$ over $\mathbb{Q}(\sqrt{8}, \sqrt{p})$ that are negative, i.e., by the parity of the number of quadratic residues $a \bmod p$ for which $0 < a < p/8$, we see that this theorem is equivalent to the version we used in Section 2 in case $q = 8$.

For $q \neq 8$, the biquadratic residue symbols are well defined with values ± 1 because of the following lemma, which is the counterpart of Theorem 1 for the case $f = qp$.

LEMMA. *For $p, q \equiv 1 \bmod 4$ odd primes one has*

$$4 \mid h_{qp}^{+} \Leftrightarrow \left(\frac{p}{q}\right) = 1;$$

$$8 \mid h_{qp}^{+} \Leftrightarrow \left(\frac{q}{p}\right)_4 = \left(\frac{\varepsilon_q}{p}\right) = 1$$

$$\Leftrightarrow \left(\frac{q}{p}\right)_4 = \left(\frac{p}{q}\right)_4 = 1.$$

Proof. The proof is almost identical to that of the case $q = 8$ treated in Theorem 1. One considers again H_4 over its subfield $\mathbb{Q}(\sqrt{q})$, and observes that this is an extension of degree 4 if and only if p splits in $\mathbb{Q}(\sqrt{p})$. This gives the criterion for $4 \mid h_{qp}^{+}$.

Assume $4 \mid h_{qp}^{+}$. Looking at the corresponding ray class group as in the proof of Theorem 1, one sees that H_4 is real if and only if $(\varepsilon_q/p) = 1$, and that the prime $(\sqrt{q})$ splits completely in it when $(\varepsilon_q\sqrt{q}/p) = 1$. Note that by symmetry $(\varepsilon_q/p) = (\varepsilon_p/q)$. One has $8 \mid h_{qp}^{+}$ exactly when H_4 is real and $(\sqrt{q})$ splits completely in it, which yields the first condition for divisibility by 8. As the product of the primes over p and q in $\mathcal{C}(qp)$ is the "Frobenius at infinity," which is trivial on H_4 if and only if H_4 is real, one has the identity

$$\left(\frac{q}{p}\right)_4\left(\frac{p}{q}\right)_4 = \left(\frac{\varepsilon_q}{p}\right) = \left(\frac{\varepsilon_p}{q}\right)$$

known as *Scholz's reciprocity law*. The second criterion is now also obvious. ∎

The proof of Theorem 4 is based on the analytic class number formula [7], which states that for a real quadratic field of discriminant f, one has $2h_f \log \varepsilon_f = -\sum_{a \bmod f} \chi(a) \log|1-\zeta_f|$. Here χ is the quadratic character of conductor f and ε_f is the fundamental unit of $\mathbb{Q}(\sqrt{f})$. By subtracting $\sum_{a \bmod f} |\chi(a)| \log|1-\zeta_f| = \log|N_{\mathbb{Q}(\zeta_f)/\mathbb{Q}}(1-\zeta_f)|$ from both sides, we obtain

$$2h_f \log \varepsilon_f - \log|N_{\mathbb{Q}(\zeta_f)/\mathbb{Q}}(1-\zeta_f)| = -2 \sum_{\chi(a)=1} \log|1-\zeta_f|.$$

As $1-\zeta_f$ is a prime element of norm f (or 2) when f is prime (or $f=8$) and a unit otherwise , one has

$$a_f \varepsilon_f^{\,h_f} = N_{\mathbb{Q}(\zeta_f)/\mathbb{Q}(\sqrt{f})}(1-\zeta_f), \tag{3}$$

where a_f equals $\sqrt{f}$ (or $\sqrt{2}$) when f is prime (or $f=8$), and $a_f = 1$ otherwise.

The proof of Theorem 4 comes down to the evaluation of the right hand side of (3) modulo $\sqrt{f}$ for $f=qp$, always under the assumption that either q, $p \equiv 1 \bmod 4$ are distinct primes that are mutual quadratic residues, or $q=8$ and $p \equiv 1 \bmod 8$ is prime. We split up the proof in two lemmas.

LEMMA 1. *One has* $N_{\mathbb{Q}(\zeta_{qp})/\mathbb{Q}(\sqrt{qp})}(1-\zeta_{qp}) = N_{\mathbb{Q}(\lambda_q,\lambda_p)/\mathbb{Q}(\sqrt{q},\sqrt{p})}(\lambda_q-\lambda_p)^4$.

Proof. As $\zeta_{qp}^{q+p} = \zeta_p\zeta_p$ and ζ_{qp} are conjugates over $\mathbb{Q}(\sqrt{q},\sqrt{p})$, we can replace ζ_{qp} by $\zeta_{qp}^{q+p} = \zeta_q\zeta_p$ in the left hand side. One easily checks the identity

$$\begin{aligned} &N_{\mathbb{Q}(\zeta_{qp})/\mathbb{Q}(\lambda_q,\lambda_p)}(1-\zeta_q\zeta_p) \\ &\quad = (1-\zeta_q\zeta_p)(1-\zeta_q^{\,-1}\zeta_p)(1-\zeta_q\zeta_p^{\,-1})(1-\zeta_q^{\,-1}\zeta_p^{\,-1}) = (\lambda_q-\lambda_p)^2, \end{aligned}$$

which reduces the proof to showing that $\alpha = N_{\mathbb{Q}(\zeta_{qp})/\mathbb{Q}(\sqrt{q},\sqrt{p})}(1-\zeta_q\zeta_p)$ is an element of $\mathbb{Q}(\sqrt{qp})$. Let σ and τ denote the non-trivial automorphisms of $\mathbb{Q}(\sqrt{q},\sqrt{p})$ over respectively $\mathbb{Q}(\sqrt{q})$ and $\mathbb{Q}(\sqrt{p})$. We will show that $\alpha^\sigma = \alpha^\tau = \alpha^{-1}$, such that α is invariant under $\sigma\tau$ and therefore in $\mathbb{Q}(\sqrt{qp})$. Indeed, we have

$$\begin{aligned} \alpha^{\sigma+1} &= N_{\mathbb{Q}(\sqrt{q},\sqrt{p})/\mathbb{Q}(\sqrt{q})}\alpha = N_{\mathbb{Q}(\zeta_{qp})/\mathbb{Q}(\sqrt{q})}(1-\zeta_q\zeta_p) \\ &= N_{\mathbb{Q}(\zeta_q)/\mathbb{Q}(\sqrt{q})}\left(\frac{\zeta_q^{\,p}-1}{\zeta_q-1}\right) = 1 \end{aligned}$$

because $\zeta_q^{\,p}$ and ζ_q are conjugate over $\mathbb{Q}(\sqrt{q})$. If $q \neq 8$, we also have $\alpha^{\tau+1}=1$ by symmetry and we are done. For $q=8$ one obtains $\alpha^{\tau+1} =$

$N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}(\sqrt{p})}((\zeta_p^8-1)/(\zeta_p^4-1))=1$ because ζ_p^8 and ζ_p^4 are conjugate over $\mathbb{Q}(\sqrt{p})$. ∎

As all powers of ε_{qp} are by definition positive, it follows from the preceding lemma and (3) that

$$\varepsilon_{qp}^{\,h_{qp}/4}=\sigma_{q,p}N_{\mathbb{Q}(\lambda_q,\lambda_p)/\mathbb{Q}(\sqrt{q},\sqrt{p})}(\lambda_q-\lambda_p). \tag{4}$$

We will now evaluate the element $x=N_{\mathbb{Q}(\lambda_q,\lambda_p)/\mathbb{Q}(\sqrt{q},\sqrt{p})}(\lambda_q-\lambda_p)$ modulo $\sqrt{qp}$ under the assumption $8\mid h_{qp}^+$.

LEMMA 2. *Suppose* $8\mid h_{qp}^+$. *Then we have* $x\equiv(\varepsilon_q^{\,h_q}\sqrt{q})^{(p-1)/4} \bmod(\sqrt{q})$. *If* $q=8$ *one also has* $x\equiv((1+3\varepsilon_p^{\,h_p}\sqrt{p})/4) \bmod(\sqrt{8})$.

Proof. Let g be the irreducible polynomial of λ_p over $\mathbb{Q}(\sqrt{p})$. As $\sqrt{p}$ is totally ramified in $\mathbb{Q}(\lambda_p)/\mathbb{Q}(\sqrt{p})$ and λ_p is a prime element over $\sqrt{p}$, the polynomial g is Eisenstein at the prime $\sqrt{p}$. Its degree is $(p-1)/4$. This gives a congruence

$$N_{\mathbb{Q}(\lambda_q,\lambda_p)/\mathbb{Q}(\lambda_q,\sqrt{p})}(\lambda_q-\lambda_p)=g(\lambda_q)\equiv\lambda_q^{(p-1)/4} \bmod(\sqrt{p})$$

in the ring of integers of $\mathbb{Q}(\lambda_q,\sqrt{p})$. Taking the norm to $\mathbb{Q}(\sqrt{q},\sqrt{p})$ yields

$$N_{\mathbb{Q}(\lambda_q,\lambda_q)/\mathbb{Q}(\sqrt{q},\sqrt{p})}(\lambda_q-\lambda_p)\equiv N_{\mathbb{Q}(\lambda_q)/\mathbb{Q}(\sqrt{q})}(\lambda_q^{(p-1)/4}) \bmod(\sqrt{q}),$$

If $q\neq 8$, the analytic class number formula (3) for $f=q$ yields

$$N_{\mathbb{Q}(\lambda_q)/\mathbb{Q}(\sqrt{q})}(\lambda_q)=N_{\mathbb{Q}(\zeta_q)/\mathbb{Q}(\sqrt{q})}(1-\zeta_q)=\varepsilon_q^{\,h_q}\sqrt{q}.$$

This also works for $q=8$ with $\sqrt{2}$ in the place of $\sqrt{q}$, and since then $2^{(p-1)/4}\equiv 1 \bmod p$ by our assumption on h_p^+, it gives in both cases the desired congruence modulo $(\sqrt{p})$. By symmetry, we also obtain a congruence modulo $(\sqrt{q})$ in case p and q are odd. However, for $q=8$ and $p\equiv 1 \bmod 8$ one has to do some extra work to obtain a congruence modulo $\sqrt{q}=2\sqrt{2}$.

Let $g=\sum_{i=1}^{n}\alpha_i X^i$ be the irreducible polynomial of λ_p over $\mathbb{Q}(\sqrt{p})$. We will show that

$$x=N_{\mathbb{Q}(\sqrt{2},\lambda_p)/\mathbb{Q}(\sqrt{2},\sqrt{p})}(\lambda_8-\lambda_p)=g(\lambda_8)\equiv\frac{1+3\alpha_0}{4} \bmod 2\sqrt{2},$$

which finishes the proof as $\alpha_0=\varepsilon_p^{\,h_p}\sqrt{p}$ by (3). Note that $\log_2\alpha_0\equiv 0 \bmod 8$ by (1) and Theorem 2. One even knows that $\alpha_0\equiv 1 \bmod 8$ as $\mathbb{Q}(\sqrt{\alpha_0})=\mathbb{Q}(\sqrt{p},\sqrt{\varepsilon_p\sqrt{p}})$ is the quartic subfield of $\mathbb{Q}(\zeta_p)$ when $p\equiv 1 \bmod 8$, and in our situation the prime 2 splits completely in this field.

In order to obtain information about the coefficients $\alpha_1, \alpha_2 \in \mathbb{Q}(\sqrt{p})$ modulo powers of $\sqrt{2}$, we evaluate

$$g(4) = N_{\mathbb{Q}(\zeta_p)\mathbb{Q}(\sqrt{p})}(2+\zeta_p+\zeta_p^{-1}) = N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}(\sqrt{p})}(1+\zeta_p)$$
$$= N_{\mathbb{Q}(\zeta_p)\mathbb{Q}(\sqrt{p})}\left(\frac{1-\zeta_p^2}{1-\zeta_p}\right) = 1,$$

which gives $g(4)-1 = 0 \equiv 4\alpha_1 + \alpha_0 - 1 \bmod 16$. We find $\alpha_1 \equiv ((1-\alpha_0)/4) \bmod 4$, and in particular $\alpha_1 \equiv 0 \bmod 2$ as $\alpha_0 \equiv 1 \bmod 8$. Further

$$g(2)^2 = N_{\mathbb{Q}(\zeta_p)\mathbb{Q}(\sqrt{p})}(\zeta_p+\zeta_p^{-1})^2 = N_{\mathbb{Q}(\zeta_p)\mathbb{Q}(\sqrt{p})}(\zeta_p+\zeta_p^{-1})$$
$$= N_{\mathbb{Q}(\zeta_p)\mathbb{Q}(\sqrt{p})}\left(\frac{\zeta_p^2-\zeta_p^{-2}}{\zeta_p-\zeta_p^{-1}}\right) = 1,$$

so $g(2) = 1$ because $g(4) - g(2) \equiv 2\alpha_1 \equiv 0 \bmod 4$. This yields $g(2) - 1 = 0 \equiv 4\alpha_2 + 2\alpha_1 + \alpha_0 - 1 \bmod 8$, so $2\alpha_2 \equiv -\alpha_1 - (\alpha_0 - 1)/2 \equiv (1-\alpha_0)/4 \bmod 4$. We conclude that

$$x = g(\lambda_8) \equiv \lambda_8^2\alpha_2 + \lambda_8\alpha_1 + \alpha_0 \equiv 2\alpha_2 + \alpha_0 \equiv \frac{1+3\alpha_0}{4} \bmod 2\sqrt{2}$$

as we wanted to show. ∎

Proof of Theorem 4. Using (3) and the preceding lemma, one obtains

$$\eta_{qp}^{h_{qp}^+/8} = \varepsilon_{qp}^{h_{qp}/4} = \lambda_{q,p} N_{\mathbb{Q}(\lambda_q,\lambda_p)/\mathbb{Q}(\sqrt{q},\sqrt{p})}(\lambda_q - \lambda_p)$$
$$\equiv (\varepsilon_q^{h_q}\sqrt{q})^{(p-1)/4} \bmod (\sqrt{p}).$$

As $1 = \mathrm{Norm}(\eta_{qp}) \equiv \eta_{qp}^2 \bmod (\sqrt{qp})$ one has $\eta_{qp} \equiv \eta_{qp}^{-1} \bmod (\sqrt{qp})$. Further h_q is odd and $(\varepsilon_p/q) = (\varepsilon_p^2/q)_4 = 1$ by the assumption $8 \mid h_{qp}^+$, so the congruence $\bmod(\sqrt{p})$ follows. If $q \neq 8$, the other congruence follows by symmetry. For $q = 8$ one uses the definition of $(\cdot/2)_4$ and the congruence modulo $\sqrt{8}$ of the lemma instead. ∎

Remark. As we have alreadty seen, these congruences may be formulated as ordinary rational congruences modulo p and q (or p and 4) by replacing η_{qp} by the element $u \in \frac{1}{2}\mathbb{Z}$ occurring in its representation on a $\mathbb{Q}$-basis $\eta_{qp} = u + v\sqrt{qp}$. If p and q are odd, there are three possible values of $(u \bmod p,\ u \bmod q)$ corresponding to whichever of the three elements -1, p, and q is an integral norm from $\mathbb{Q}(\sqrt{qp})$.

4. Density Statements

It follows from Theorem 1 and Čebotarev's density theorem that the sets of prime numbers $p \equiv 1 \bmod 4$ for which any of the three class numbers h_{4p}, h_{8p}, and h_{8p}^+ is divisible by 4 or 8 have natural densities. More precisely, the natural density of the set of primes $p \equiv 1 \bmod 4$ for which $a \mid h_f^+$ is given by the diagram

a	$f = 8p$	$f = -8p$	$f = -4p$
4	1/4	1/4	1/4
8	1/16	1/8	1/8
2^n	4^{1-n}	2^{-n}	2^{-n}

in which the densities in the last line have only been determined for $n \leqslant 3$. It seems reasonable to expect that these density statements are true for $n \geqslant 4$ as well. However, the only way so far to prove such results has been the construction of a governing field for the corresponding 2^n-rank. In our three cases these are metabelian extensions of $\mathbb{Q}$ of degree 8 or 16 that are unramified outside 2 and ∞. Such constructions break down for $n \geqslant 4$ because the 8-Hilbert class fields one would need are no longer abelian over some base field independent of p. The unit criteria such as the one in Theorem 2 do not directly lead to a governing field. One sees that, rather than being determined by the splitting behaviour of p in some number field of degree 16 unramified outside $2 \cdot \infty$, the divisibility of h_{4p} by 16 depends on the splitting behaviour of 2 in a normal extension $F_p = \mathbb{Q}(\zeta_8, \sqrt[4]{p\varepsilon_p})$ of degree 16 depending on p. In this case, the problem comes down to finding a field governing the 2-adic behaviour of ε_p, which appears to be hard.

By looking at Theorem 3 and the theorem at the end of Section 2, one sees that the existence of governing fields for the 16-rank of $\mathcal{C}(-4p)$ and $\mathcal{C}(-8p)$ implies the existence of a governing field for the 16-rank of $\mathcal{C}(8p)$ and conversely. The compositum of such hypothetical fields would necessarily govern the value of E_{8p} in case 16 does not divide h_{8p}^+. Such a situation is already familiar to us in case $8 \nmid h_{8p}^+$, when the character values of $\chi(\zeta_8)$ and $\chi(1+\zeta_8^2)$ for the prime p occurring in Theorem 1 are not both equal to 1 and determine E_{8p} as follows.

Lemma. *Let ζ_8 be a primitive 8th root of unity in the field of p elements, and χ the quadratic character of conductor p. Then we have*

$$\chi(\zeta_8) = -1 \quad \text{and} \quad \chi(1+\zeta_8^2) = 1 \Rightarrow E_{8p} = -1;$$

$$\chi(\zeta_8) = 1 \quad \text{and} \quad \chi(1+\zeta_8^2) = -1 \Rightarrow E_{8p} = 2;$$

$$\chi(\zeta_8) = -1 \quad \text{and} \quad \chi(1+\zeta_8^2) = -1 \Rightarrow E_{8p} = -2.$$

If $\chi(\zeta_8) = \chi(1+\zeta_8^2) = 1$ then all three values of E_{8p} can occur.

Proof. The implications in the lemma follow immediately from the following implications, of which the first two go back to Dirichlet.

$$E_{8p} = \quad 2 \Rightarrow \chi(\zeta_8) = 1;$$
$$E_{8p} = -2 \Rightarrow \chi(\zeta_8)\,\chi(1+\zeta_8^2) = 1;$$
$$E_{8p} = -1 \Rightarrow \chi(1+\zeta_8^2) = 1.$$

We include the elementary proofs of these results for the convenience of the reader.

If $E_{8p} = a^2 - 2pb^2 = 2$, we have $pb^2 \equiv 1 \bmod 16$. As 2 is a square modulo each prime dividing b, we have $b^2 \equiv 1 \bmod 16$, so $p \equiv 1 \bmod 16$.

If $a^2 - 2pb^2 = -2$, then a is a square root of -2 modulo p, so we can assume $a \bmod p = \zeta_8 + \zeta_8^3$. For any odd prime $q \mid a$, we have $\chi(q) = (p/q) = (pb^2/q) = (1/q) = 1$. As also $\chi(2) = 1$, it follows that $\chi(a) = 1$, as is to be shown.

Finally, if $E_{8p} = u^2 - 2pv^2 = -1$, we have $\chi(1+\zeta_8^2) = \chi(1+u)$. For any odd prime divisor q of $1+u$, we have $\chi(q) = (p/q) = (2pv^2/q)(2/q) = ((u^2+1)/q)(2/q) = (2/q)(2/q) = 1$. As before we conclude that $\chi(1+u) = 1$.

In case $\chi(\zeta_8) = \chi(1+\zeta_8^2) = 1$ the implications above do not exclude a value of E_{8p}. The examples $p = 113$, 337, and 257 give respectively $E_{8p} = -1$, 2, and -2, so all three cases do indeed occur. ∎

The hypothetical governing field for the 16-rank of our class groups would imply a result analogous to the preceding lemma for the set of

TABLE I

Distribution of 16-ranks $r_{16}(f)$ for $f = 8p$, $-8p$, and $-4p$ for primes $p < 10^6$ satisfying $8 \mid h_{8p}^*$.

$r_{16}(8p)$	$r_{16}(-8p)$	$r_{16}(-4p)$	δ	E_{8p}	# of primes		24 × frac.	
				-1	210		1.03	
1	1	1	+1	+2	179	581	0.88	2.86
				-2	192		0.95	
				-1	190		0.94	
1	1	0	-1	+2	186	579	0.92	2.85
				-2	203		1.00	
	0	1		-1	605		2.98	
0	0	0	+1	+2	619	1827	3.05	9.00
	1	0		-2	603		2.97	
	0	0		-1	631		3.11	
0	0	1	-1	2	643	1885	3.17	9.29
	1	1		-2	611		3.01	

primes for which $\chi(\zeta_8)=\chi(1+\zeta_8^2)=1$, since E_{8p} is determined by $\delta=\chi(1+\zeta_8)$ and the 16-rank of $\mathcal{C}(-4p)$ and $C(-8p)$ in case $8\|h_{8p}^+$, and all three possibilities occur when $16|h_{8p}^+$. More generally, one is led to expect each of the three values of E_{8p} to occur with proportion $\sum_{n\geq 1}4^{-n}=\frac{1}{3}$ among the primes $p\equiv 1 \bmod 8$. This agrees with the numerical observations in Table I.

Table I, which was compiled with the help of the PARI-calculator, gives the distribution of the 16-ranks of $\mathcal{C}(8p)$, $\mathcal{C}(-8p)$, and $\mathcal{C}(-4p)$ for the 4872 prime numbers $p<10^6$ for which the three 8-ranks equal 1. The set of these primes has density 1/16 by Theorem 1. It splits up in two halves corresponding to the two values of $\delta=\chi(1+\zeta_8)$, and one sees that the three values of E_{8p} seem to be equally probable on those halves. In each of the six cases, one has $16|h_{8p}^+$ for approximately $\frac{1}{4}$ of the primes. In each of the 12 cases thus obtained, h_{8p} and h_{-4p} are determined modulo 16 by the theorems proved in Section 2. In order to compare the results to the expected values, which are 1/24 for the six cases having $16|h_{8p}^+$ and 1/8 for the six remaining cases, we have given the values of the fraction of the number of primes corresponding to each case, multiplied by 24.

References

1. P. Barrucand and H. Cohn, Primes of type x^2+32y^2, class number and residuacity, *J. Reine Angew. Math.* **238** (1969), 67–70.
2. E. Brown, The class number of $\mathbb{Q}(\sqrt{-p})$, for $p\equiv 1 \bmod 8$ a prime, *Proc. Amer. Math. Soc.* **31** (1972), 381–383.
3. J. Bucher, Neues über die Pellsche Gleichung, *Mitt. Natur. Ges. Luzern* **14** (1943), 1–18.
4. D. A. Buell and K. S. Williams, An octic reciprocity law of Scholz type, *Proc. Amer. Math. Soc.* **77**, No. 3 (1979), 315–318.
5. H. Cohn, The explicit Hilbert 2-cyclic class field for $\mathbb{Q}(\sqrt{-p})$, *J. Reine Angew. Math.* **321** (1981), 64–77.
6. H. Cohn and J. C. Lagarias, On the existence of fields governing the 2-invariants of the class groups of $\mathbb{Q}(\sqrt{dp})$ as p varies, *Math. Comp.* **41** (1983), 711–730.
7. H. Davenport, Multiplicative number theory, *Springer GTM* **74** (1967, revised ed. 1980).
8. C. F. Gauss, "De nexu inter multitudinem classum, in quas formae binariae secundi gradus distribuuntur, earumque determinantem," Werke, Vol. II, pp. 269–305, Kön. Ges. der Wissenschaften, Göttingen, 1876.
9. G. Gras, Relations congruentielles linéaires entre nombres de classes de corps quadratiques, *Acta Arith.* **52** (1989), 147–162.
10. K. Hardy and K. S. Williams, A congruence relating the class numbers of complex quadratic fields, *Acta Arith.* **47** (1986), 263–276.
11. H. Hasse, Über die Klassenzahl des Körpers $P(\sqrt{-p})$ mit einer Primzahl $p\equiv(1 \bmod 2^3)$, *Aequationes Math.* **3** (1969), 165–169.
12. H. Hasse, Über die Klassenzahl des Körpers $P(\sqrt{-2p})$ mit einer Primzahl $p\neq 2$, *J. Number Theory* **1** (1969), 231–234.
13. H. Hasse, Über die Teilbarkeit durch 2^3 der Klassenzahl imaginärquadratischer Zahlkörper mit genau zwei verschiedenen Diskriminantenprimteilern, *J. Reine Angew. Math.* **241** (1970), 1–6.

14. H. HASSE, Über die Teilbarkeit durch 2^3 der Klassenzahl der quadratischen Zahlkörper mit genau zwei verschiedenen Diskriminantenprimteilern, *Math. Nachr.* **46** (1970), 61–70.
15. P. KAPLAN, Divisibilité par 8 du nombre des classes des corps quadratiques dont le 2-groupe des classes est cyclique, et réciprocité biquadratique, *J. Math. Soc. Japan* **25** (1973), 596–608.
16. P. KAPLAN, Sur le 2-groupe des classes d'idéaux des corps quadratiques, *J. Reine Angew. Math.* **283/284** (1976), 313–363.
17. P. KAPLAN, K. HARDY, AND K. S. WILLIAMS, Divisibilité par 16 du nombre des classes au sens strict des corps quadratiques réels dont le deux-groupe des classes est cyclique, *Osaka J. Math.* **23** (1986), 479–489.
18. P. KAPLAN AND K. S. WILLIAMS, On the class numbers of $\mathbb{Q}(\sqrt{\pm 2p})$ modulo 16, for $p \equiv 1 \bmod 8$ a prime, *Acta Arith.* **40** (1982), 289–296.
19. P. KAPLAN AND K. S. WILLIAMS, On the strict class number of $\mathbb{Q}(\sqrt{2p})$ modulo 16, $p \equiv 1 \bmod 8$ a prime, *Osaka J. Math.* **21** (1984), 23–29.
20. H. KOCH AND W. ZINK, Über die 2-Komponente der Klassengruppe quadratischer Zahlkörper mit zwei Diskriminantenteilern, *Math. Nachr.* **54** (1972), 309–333.
21. P. A. LEONARD AND K. S. WILLIAMS, On the divisibility of the class numbers of $\mathbb{Q}(\sqrt{-p})$ and $\mathbb{Q}(\sqrt{-2p})$ by 16, *Canad. Math. Bull.* **25** (1982), 200–206.
22. P. MORTON, The quadratic number fields with cyclic 2-class groups, *Pacific J. Math.* **108** (1983), 165–175.
23. B. ORIAT, Sur la divisibilité par 8 et 16 des nombres de classes d'idéaux des corps quadratiques $\mathbb{Q}(\sqrt{2p})$ et $\mathbb{Q}(\sqrt{-2p})$, *J. Math. Soc. Japan* **30** (1978), 279–285.
24. L. RÉDEI, Arithmetischer Beweis des Satzes über die Anzahl der durch vier teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper, *J. Reine Angew. Math.* **171** (1935), 55–60.
25. P. STEVENHAGEN, "Class Groups and Governing Fields," Thesis, UC Berkeley, Berkeley, 1988.
26. K. S. WILLIAMS, On the class number of $\mathbb{Q}(\sqrt{-p})$ modulo 16, for $p \equiv 1 \bmod 8$ a prime, *Acta Arith.* **39** (1981), 381–398.
27. Y. YAMAMOTO, Divisibility by 16 of class numbers of quadratic fields whose 2-class groups are cyclic, *Osaka J. Math.* **21** (1984), 1–22.