Compositio Mathematica **119:** 1–11, 1999.

Indivisibility of Class Numbers of Real Quadratic Fields

To T. Ono, my father, on his seventieth birthday

KEN ONO*
Department of Mathematics, Penn. State University, University Park, PA 16802 U.S.A.
e-mail: ono@math.psu.edu

(Received: 18 December 1997; accepted in final form: 28 May 1998)

Abstract. Let D denote the fundamental discriminant of a real quadratic field, and let $h(D)$ denote its associated class number. If p is prime, then the 'Cohen and Lenstra Heuristics' give a probability that $p \nmid h(D)$. If $p > 3$ is prime, then subject to a mild condition, we show that

$$\#\{0 < D < X | p \nmid h(D)\} \gg_p \frac{\sqrt{X}}{\log X}.$$

This condition holds for each $3 < p < 5000$.

Mathematics Subject Classifications (1991): Primary: 11R29; Secondary: 11E41.

Key words: class numbers of real quadratic fields.

1. Introduction and Statement of Results

Although the literature on class numbers of quadratic fields is quite extensive, very little is known. In this paper we consider class numbers of real quadratic fields, and as an immediate consequence we obtain an estimate for the number of vanishing Iwasawa λ invariants.

Throughout D will denote the fundamental discriminant of the quadratic number field $\mathbb{Q}(\sqrt{D})$, $h(D)$ its class number, and $\chi_D := (\frac{D}{\cdot})$ the usual Kronecker character. We shall let χ_0 denote the trivial character, and $|\cdot|_p$ the usual multiplicative p-adic valuation normalized so that $|p|_p := 1/p$.

Although the 'Cohen–Lenstra Heuristics' [C-L] have gone a long way towards an explanation of experimental observations of such class numbers, very little has been proved. For example, it is not known that there are infinitely many $D > 0$ for which $h(D) = 1$. The presence of nontrivial units in $\mathbb{Q}(\sqrt{D})$ have posed the main difficulty. Basically, if $\epsilon(D)$ is the fundamental unit of $\mathbb{Q}(\sqrt{D})$, then the regulator $R(D) := \log(\epsilon(D))$ complicates Dirichlet's class number formula

$$L(1, \chi_D) = \frac{2h(D)R(D)}{\sqrt{D}},$$

* The author is supported by NSF grant DMS-9508976 and NSA grant MSPR-97Y012.

one of the main vehicles for studying $h(D)$.

In view of these and other difficulties, it is natural to ask how often $p \nmid h(D)$, given a prime p. For the complementary question, M. R. Murty [M] has recently obtained lower bounds, although far from the Cohen and Lenstra expectation, for the number of D, both negative and positive, for which $p|h(D)$. His results extend work of Ankeny and Chowla, Humbert, and Nagell where explicit elements of order p were constructed for infinitely many discriminants.

For $D > 0$, Cohen and Lenstra predict that the 'probability' $p \nmid h(D)$ is

$$\left(\frac{p}{p-1}\right)\prod_{i=1}^{\infty}(1-p^{-i}) = 1 - \frac{1}{p^2} - \frac{1}{p^3} - \frac{1}{p^4} + \cdots,$$

and for $D < 0$ they conjecture that the 'probability' is

$$\prod_{i=1}^{\infty}(1-p^{-i}) = 1 - \frac{1}{p} - \frac{1}{p^2} + \frac{1}{p^5} + \cdots.$$

Although extensive numerical evidence lends credence to these heuristics, apart from the works of Davenport and Heilbronn [D-H] when $p = 3$, little has been proved.

Imaginary quadratic fields have been the focus of numerous investigations in this direction. For instance, one may see the works of Hartung [Ha], Horie and Onishi [Ho, Ho1, Ho-On], Jochnowitz [J], and Ono and Skinner [O-Sk]. These papers guarantee, under various conditions, that there are indeed infinitely many $D < 0$ for which $p \nmid h(D)$. In a recent paper, the author and Kohnen [Koh-O] have gone a step further by obtaining a lower bound for the number of $-X < D < 0$ for which $p \nmid h(D)$. In particular if p is prime and $\epsilon > 0$, then for all sufficiently large $X > 0$

$$\#\{-X < D < 0 \,|\, h(D) \not\equiv 0 (\mathrm{mod}\, p)\} \geqslant \left(\frac{2(p-2)}{\sqrt{3}(p-1)} - \epsilon\right)\frac{\sqrt{X}}{\log X}.$$

Even less is known about the indivisibility of class numbers of real quadratic fields. There is work in this direction by Jochnowitz [J]. Subject to a mild condition regarding the existence of a suitable generalized Bernoulli number $B((p-1)/2, \chi)$, we go a step further by obtaining a lower bound for the number of $0 < D < X$ for which $p \nmid h(D)$. As in [J], we also obtain information about $R_p(D)$, the p-adic regulator of $\mathbb{Q}(\sqrt{D})$.

THEOREM 1. *Let $p > 3$ be prime. If there is a fundamental discriminant D_0 coprime to p for which*

(i) $(-1)^{(p-1)/2}D_0 > 0$,

(ii) $\left|B\left(\frac{p-1}{2}, \chi_{D_0}\right)\right|_p = 1$,

then

$$\#\left\{0 < D < X \mid h(D) \not\equiv 0 (\mathrm{mod}\ p),\ p|D, \textit{and} \left|\frac{R_p(D)}{\sqrt{D}}\right|_p = 1\right\} \gg_p \frac{\sqrt{X}}{\log X}.$$

A lengthy MAPLE computation yields the following immediate corollary.

COROLLARY 1. *If* $3 < p < 5000$ *is prime, then*

$$\#\left\{0 < D < X \mid h(D) \not\equiv 0 (\mathrm{mod}\ p),\ p|D, \textit{and} \left|\frac{R_p(D)}{\sqrt{D}}\right|_p = 1\right\} \gg_p \frac{\sqrt{X}}{\log X}.$$

This gives some evidence for a conjecture of Greenberg on Iwasawa invariants [G]. Let $K = K_0$ be a number field, and let p be an odd prime. If $\mathbb{Q}_n$ denotes the unique subfield of degree p^n in the field $\mathbb{Q}(\zeta_{p^{n+1}})$, the field of the p^{n+1}th roots of unity, then let $K_n := K\mathbb{Q}_n$. These define the $\mathbb{Z}_p$ cyclotomic extension of K $K = K_0 \subset K_1 \subset K_2 \ldots$. If Cl_n denotes the p-part of the class group of K_n, then $Cl_0 \leftarrow Cl_1 \leftarrow Cl_2 \leftarrow \cdots$ where each map is a norm. Iwasawa [Thm. 13.13, W] proved that if n is sufficiently large, then $\#Cl_n = p^{\mu(K,p)p^n + \lambda(K,p)n + \nu(K,p)}$, where $\mu(K, p)$, $\lambda(K, p)$, and $\nu(K, p)$ are fixed integers, the 'Iwasawa invariants'.

If $K = \mathbb{Q}(\sqrt{D})$ is a real quadratic field, then Greenberg's Conjectures [G] imply that $\lambda(\mathbb{Q}(\sqrt{D}), p) = \mu(\mathbb{Q}(\sqrt{D}), p) = 0$. By a theorem of Ferrero and Washington, it is indeed known that $\mu(\mathbb{Q}(\sqrt{D}), p) = 0$, but the complementary question regarding the vanishing of $\lambda(D, p) := \lambda(\mathbb{Q}(\sqrt{D}), p)$ remains open.

For $p = 3$, Horie and Nakagawa [Ho-N] used a theorem of Davenport and Heilbronn [D-H] and a criterion of Iwasawa to show that $\lambda(D, 3) = 0$ for a positive 'proportion' of D. Moreover, recent calculations for $D < 10000$ by Kraft and Schoof [K-S], Fukuda and Taya [F-T], and Ichimura and Sumida [Ic-Su] verify indeed that $\lambda(D, 3) = 0$ for all $D < 10^4$. Less is known when $p > 3$. Corollary 1 implies the following immediate result.

COROLLARY 2. *If* $3 < p < 5000$ *is prime, then*

$$\#\{0 < D < X \mid \lambda(D, p) = 0\} \gg_p \frac{\sqrt{X}}{\log X}.$$

In Section 2 we shall present the essential preliminaries, and in Section 3 we shall prove these results.

2. Preliminaries

H. Cohen [C] explicitly constructed half-integral weight Eisenstein series whose Fourier coefficients are given by generalized Bernoulli numbers for quadratic characters. These modular forms play a crucial role in this paper. Consult [Ko] for definitions and the standard facts about modular forms.

Fix an integer $r \geqslant 2$. If $N \not\equiv 0, 1 (\mathrm{mod}\, 4)$, then let $H(r, N) := 0$. If $N = 0$, then let $H(r, 0) := \zeta(1-2r) = -B_{2r}/2r$. If N is a positive integer and $Dn^2 = (-1)^r N$ where D is the fundamental discriminant of a quadratic number field, then define $H(r, N)$ by

$$H(r, N) := L(1-r, \chi_D) \sum_{d|n} \mu(d)\chi_D(d) d^{r-1} \sigma_{2r-1}(n/d). \tag{1}$$

As usual $\sigma_\nu(n) := \sum_{d|n} d^\nu$. In particular, if $D = (-1)^r N$ is the discriminant of a quadratic number field, then

$$H(r, N) = L(1-r, \chi_D) = -\frac{B(r, \chi_D)}{r}, \tag{2}$$

where $B(n, \chi)$ is the nth generalized Bernoulli number with character χ. If $(-1)^r N = n^2$, then

$$H(r, N) = \zeta(1-r) \sum_{d|n} \mu(d) d^{r-1} \sigma_{2r-1}(n/d). \tag{3}$$

PROPOSITION 1 [Thm. 3.1, C]. *If $r \geqslant 2$ and $F_r(z) := \sum_{n=0}^{\infty} H(r, N) q^N$ ($q := \mathrm{e}^{2\pi i z}$), then $F_r(z) \in M_{r+1/2}(\Gamma_0(4), \chi_0)$.*

If $D > 0$, then let $L_p(s, \chi_D)$ denote the Kubota–Leopoldt p-adic Dirichlet L-function with character χ_D, and let $R_p(D)$ denote the p-adic regulator of $\mathbb{Q}(\sqrt{D})$ [Ch. 5, W].

PROPOSITION 2. *If $p > 3$ is prime and D is a fundamental discriminant coprime to p for which $(-1)^{(p-1)/2} D > 0$, then $H((p-1)/2, D)$ is p-integral and*

$$H\left(\frac{p-1}{2}, D\right) \equiv \frac{2h(D_p) R_p(D_p)}{\sqrt{D_p}} (\mathrm{mod}\, p),$$

where $D_p := (-1)^{(p-1)/2} Dp$.

Proof. By (2) we find that $H((p-1)/2, D) = L(1-(p-1)/2, \chi_D) = -2B((p-1)/2, \chi_D)/(p-1)$, and it is well known to be p-integral by a theorem of Carlitz [Ca].

Now D_p is a positive fundamental discriminant, and by the construction of the Kubota–Leopoldt p-adic L-function $L_p(s, \chi_D)$ [Thm. 5.11, W]

$$L_p\left(1 - \frac{p-1}{2}, \chi_{D_p}\right) = -\frac{2B(\frac{p-1}{2}, \chi_{D_p} \cdot \omega^{-(p-1)/2})}{p-1},$$

where ω is the usual Teichmüller character. It is easy to see that $\chi_{D_p} \cdot \omega^{-(p-1)/2} = \chi_D$, and so

$$L_p\left(1 - \frac{p-1}{2}, \chi_{D_p}\right) = -\frac{2B(\frac{p-1}{2}, \chi_D)}{p-1} = H\left(\frac{p-1}{2}, D\right).$$

By the Kummer congruences [Cor. 5.13, W], we find that $L_p(1, \chi_{D_p}) \equiv L_p(1-(p-1)/2, \chi_{D_p}) \pmod p$, and so the claim now follows from the p-adic class number formula [Thm. 5.24, W]

$$L_p(1, \chi_{D_p}) = \frac{2h(D_p)R_p(D_p)}{\sqrt{D_p}}. \qquad \square$$

Remark 1. Although one might suspect that the Eisenstein series $F_{p-1}(z)$ would be better to work with, the obvious generalization of the proof of Theorem 1 does not work.

In view of Proposition 2, our main objective is to study its coefficients $H((p-1)/2, D) \pmod p$. Unfortunately there is a minor technical difficulty which arises. The coefficients $H((p-1)/2, 0)$ and $H((p-1)/2, pn^2)$ are not p-integral. However this does not pose too much trouble as the next two propositions indicate.

PROPOSITION 3. *If $p > 3$ is prime, then there exists an integer $\alpha(p)$ coprime to p for which*

(i) $\alpha(p)pF_{(p-1)/2}(z) \in \mathbb{Z}[[q]]$,

(ii) $\alpha(p)pF_{(p-1)/2}(z) \equiv \Theta(pz) \pmod p$,

where $\Theta(z) := \sum_{n=-\infty}^{\infty} q^{n^2} = 1 + 2q + 2q^4 + 2q^9 + \cdots \in M_{1/2}(\Gamma_0(4), \chi_0)$.

Proof. By (1), (2), and a theorem of Carlitz [Ca], it turns out that the only coefficients of $F_{(p-1)/2}(z)$ which are not necessarily p-integral are $H((p-1)/2, 0)$ and $H((p-1)/2, pn^2)$. Therefore if $n \neq p\square$, then $pH((p-1)/2, n) \equiv 0 \pmod p$.

Since

$$H\left(\frac{p-1}{2}, 0\right) = \zeta(1-(p-1)) = -\frac{B_{p-1}}{p-1},$$

$$H\left(\frac{p-1}{2}, p\right) = L\left(1 - \frac{p-1}{2}, \Psi_p\right) = -\frac{2B(\frac{p-1}{2}, \Psi_p)}{p-1},$$

where Ψ_p is the Kronecker Dirichlet character for $\mathbb{Q}(\sqrt{(-1)^{(p-1)/2}p})$, the proof now follows from (1) and the Claussen and Von Staudt theorem [Thm. 5.10, W] once one checks that

$$\frac{H\left(\frac{p-1}{2}, p\right)}{H\left(\frac{p-1}{2}, 0\right)} \equiv 2 \pmod p,$$

and

$$\sum_{d|n} \mu(d)\Psi_p(d)d^{(p-3)/2}\sigma_{p-2}(n/d) \equiv 1 \pmod{p}.$$

The second congruence follows easily, and the first congruence follows easily from the definitions of Bernoulli numbers and generalized Bernoulli numbers. □

3. Proof of Results

Theorem 1 follows easily from the following result.

THEOREM 2. *Let $p > 3$ be prime, and suppose there is a fundamental discriminant D_0 coprime to p for which*

(i) $(-1)^{(p-1)/2}D_0 > 0$,

(ii) $\left| B\left(\frac{p-1}{2}, \chi_{D_0}\right)\right|_p = 1.$

Then there is an arithmetic progression $r_p \pmod{t_p}$ with $(r_p, t_p) = 1$, and a constant $\kappa(p)$ such that for each prime $\ell \equiv r_p \pmod{t_p}$ there is an integer $1 \leqslant d_\ell \leqslant \kappa(p)\ell$ for which

(i) $D_\ell := d_\ell \ell p$ *is a fundamental discriminant*,

(ii) $h(D_\ell) \not\equiv 0 \pmod{p}$,

(iii) $\left|\frac{R_p(D_\ell)}{\sqrt{D_\ell}}\right|_p = 1.$

Proof of Theorem 2. Fix at the outset an integer $\alpha(p)$ satisfying the conditions of Proposition 3. Define $\mathfrak{F}_p(z) \in M_{p/2}(\Gamma_0(4p^2), \chi_0)$ by

$$\begin{aligned}\mathfrak{F}_p(z) &:= \alpha(p)F_{(p-1)/2}(z) - \alpha(p)\left(V_p|U_p|F_{(p-1)/2}\right)(z)\\ &= \alpha(p)\sum_{(n,p)=1} H\left(\frac{p-1}{2}, n\right)q^n.\end{aligned}$$

Let $Q \neq p$ be any prime for which $(D_0/Q) = -1$, and define $\mathfrak{G}_p(z) \in M_{p/2}(\Gamma_0(4p^2Q^2), \chi_0)$ by

$$\mathfrak{G}_p(z) := \mathfrak{F}_p(z) \otimes \left(\frac{\cdot}{Q}\right) = \alpha(p)\sum_{(n,p)=1}\left(\frac{n}{Q}\right)H\left(\frac{p-1}{2}, n\right)q^n.$$

Finally define $G_p(z) \in M_{p/2}(\Gamma_0(4p^2Q^4), \chi_0)$ by

$$G_p(z) := \frac{\mathfrak{G}_p(z) \otimes \left(\frac{\cdot}{Q}\right) - \mathfrak{G}_p(z)}{2}$$

$$= \alpha(p) \sum_{(n,p)=1,(n/Q)=-1} H\left(\frac{p-1}{2}, n\right) q^n. \tag{4}$$

It is easy to see that $0 \not\equiv G_p(z) \pmod{p}$ since the coefficient of q^{D_0} in $G_p(z)$ is nonzero by hypothesis. Moreover the coefficients

$$H((p-1)/2, 0), \qquad H((p-1)/2, n^2) \quad \text{and} \quad H((p-1)/2, pn),$$

among others, have been annihilated. In particular, by (1), Proposition 2, and Proposition 3 every remaining nonzero coefficient is p-integral and contains information about the class number and p-adic regulator of some real quadratic field in which p ramifies.

If ℓ is prime, then define $(U_\ell|G_p)(z)$ and $(V_\ell|G_p)(z) \in M_{p/2}(\Gamma_0(4p^2Q^4\ell), (\frac{4\ell}{\cdot})$ in the usual way (see [Sh]), i.e.

$$(U_\ell|G_p)(z) := \sum_{n=1}^{\infty} u_{p,\ell}(n) q^n$$

$$= \alpha(p) \sum_{\left(\frac{\ell n}{Q}\right)=-1, \left(\frac{\ell n}{p}\right)=1} H\left(\frac{p-1}{2}, \ell n\right) q^n, \tag{5a}$$

$$(V_\ell|G_p)(z) := \sum_{n=1}^{\infty} v_{p,\ell}(n) q^n$$

$$= \alpha(p) \sum_{\left(\frac{n}{Q}\right)=-1, \left(\frac{n}{p}\right)=1} H\left(\frac{p-1}{2}, n\right) q^{\ell n}. \tag{5b}$$

If $g = \sum_{n=0}^{\infty} a(n) q^n$ has integer coefficients, then define $\operatorname{ord}_p(g)$ by

$$\operatorname{ord}_p(g) := \min\{n | a(n) \not\equiv 0 \pmod{p}\}.$$

By a theorem of Sturm [St], if $g \in M_k(\Gamma_0(N), \chi)$ has integer coefficients and

$$\operatorname{ord}_p(g) > \frac{k}{12}[\Gamma_0(1) : \Gamma_0(N)],$$

then $g \equiv 0 (\mathrm{mod}\ p)$. He proved this for integral k and trivial χ, but the general case obviously follows by taking an appropriate power of g. Define $\kappa(p)$ by

$$\kappa(p) := p^2 Q^3 (p+1)(Q+1)/4.$$

Since $[\Gamma_0(1): \Gamma_0(4p^2Q^4\ell)] = 6pQ^3(p+1)(Q+1)(\ell+1)$, if ℓ is sufficiently large and $g \in M_{p/2}(\Gamma_0(4p^2Q^4\ell), (\frac{4\ell}{\cdot}))$ has integer coefficients and has the property that

$$\mathrm{ord}_p(g) > \kappa(p)\ell, \tag{6}$$

then by Sturm's theorem $g \equiv 0 (\mathrm{mod}\ p)$.

Suppose that $\ell \neq p$ is a prime for which $(\frac{\ell}{Q}) = 1$. If $(\frac{n}{Q}) \neq -1$ or $(n, p) \neq 1$, then by (5a) and (5b)

$$u_{p,\ell}(n\ell) = v_{p,\ell}(n\ell) = 0. \tag{7}$$

For those n with $(\frac{n}{Q}) = -1$ and $(n, p) = 1$

$$u_{p,\ell}(n\ell) = \alpha(p) H\left(\frac{p-1}{2}, n\ell^2\right), \tag{8a}$$

$$v_{p,\ell}(n\ell) = \alpha(p) H\left(\frac{p-1}{2}, n\right). \tag{8b}$$

If ℓ is sufficiently large for which $(\frac{\ell}{Q}) = 1$, then by (1), (4), (7) and (8a) we find for every $n \leqslant \kappa(p)$ that

$$u_{p,\ell}(n\ell) = \alpha(p)(1 - \chi_{D_n}(\ell)\ell^{(p-3)/2} + \ell^{p-2}) H\left(\frac{p-1}{2}, n\right). \tag{9}$$

Here D_n denotes the fundamental discriminant of the field $\mathbb{Q}(\sqrt{(-1)^{(p-1)/2}n})$.

Let S_p denote the set of those D_n with $n \leqslant \kappa(p)$ for which $(\frac{n}{Q}) = -1$ and $(n, p) = 1$. For all other D_n with $n \leqslant \kappa(p)$ it is clear the the coefficients of $q^{D_n m^2}$ in $G_p(z)$ are zero, and so they do not play a role in the ensuing analysis. There is a progression $r_p (\mathrm{mod}\, t_p)$ with $(r_p, t_p) = 1$ and $p | t_p$ for which

(i) $\chi_{D_n}(\ell) = 1$ for every prime $\ell \equiv r_p (\mathrm{mod}\, t_p)$ and $D_n \in S_p$,

(ii) $\left(\frac{\ell}{Q}\right) = 1$ for every prime $\ell \equiv r_p (\mathrm{mod}\, t_p)$,

(iii) $\left(\frac{r_p}{p}\right) = -1$. (10)

By (8a), (8b) and (9), for every prime $\ell \equiv r_p \ (\mathrm{mod}\, t_p)$ we find that

$$u_{p,\ell}(n\ell) \equiv \alpha(p)(1 - r_p^{(p-3)/2} + r_p^{p-2}) v_{p,\ell}(n\ell) (\mathrm{mod}\ p),$$

for all $n \leqslant \kappa(p)$. Since $v_{p,\ell}(n) = 0$ if $\ell \nmid n$, by (6) if there are no $n \leqslant \kappa(p)\ell$ coprime to ℓ for which

$$u_{p,\ell}(n) = \alpha(p)H\left(\frac{p-1}{2}, n\ell\right) \not\equiv 0 \pmod{p},$$

then $U_\ell|G_p \equiv \alpha(p)(1 - r_p^{(p-3)/2} + r_{p-2})V_\ell|G_p \pmod{p}$.

By (1), the multiplicative property for $H(r, N)$, and the definition of $u_{p,\ell}(N)$ and $v_{p,\ell}(N)$, if $\ell \equiv r_p \pmod{t_p}$, then

$$u_{p,\ell}(D_0\ell^3) \equiv \alpha(p)(1 - r_p^{(p-3)/2} - r_p^{(p-5)/2} + r_p^{p-2} + r_p^{p-3}) \times \times H\left(\frac{p-1}{2}, D_0\right) \pmod{p},$$

$$v_{p,\ell}(D_0\ell^3) \equiv \alpha(p)(1 - r_p^{(p-3)/2} + r_p^{p-2})H\left(\frac{p-1}{2}, D_0\right) \pmod{p}.$$

Since $\alpha(p)H(p-1, D_0) \not\equiv 0 \pmod{p}$, we find that $u_{p,\ell}(D_0\ell^3) \not\equiv v_{p,\ell}(D_0\ell^3) \pmod{p}$ if and only if

$$r_p^{p-3} \not\equiv r_p^{(p-5)/2} \pmod{p}.$$

This is obviously satisfied in view of (10). Therefore

$$U_\ell|G_p \not\equiv V_\ell|G_p \pmod{p},$$

and so there must be an integer $1 \leqslant n \leqslant \kappa(p)\ell$ coprime to ℓ for which

$$u_{p,\ell}(n) = \alpha(p)H\left(\frac{p-1}{2}, n\ell\right) \not\equiv 0 \pmod{p}.$$

By (1) and Proposition 2 there is a positive fundamental discriminant $D_\ell := d_\ell\ell p$ with $d_\ell \leqslant \kappa(p)\ell$ for which

$$\frac{2h(D_\ell)R_p(D_\ell)}{\sqrt{D_\ell}} \not\equiv 0 \pmod{p}.$$

The proof is now complete in view of a theorem of Coates [p. 78,W] that asserts that

$$\left|\frac{R_p(D_\ell)}{\sqrt{D_\ell}}\right|_p \leqslant 1. \qquad \square$$

Proof of Theorem 1. In the notation from Theorem 2, if $\ell \equiv r_p \pmod{t_p}$ is prime, then there is an integer $1 \leqslant d_\ell \leqslant \kappa(p)\ell$ for which $D_\ell := d_\ell\ell p$ is a

fundamental discriminant with the desired properties. Let ℓ_i denote these primes in increasing order. If $j < k < l$ and $D_{\ell_j} = D_{\ell_k} = D_{\ell_l}$, then $\ell_j\ell_k\ell_l | D_{\ell_j}$. However this can only occur for finitely many j, k, and l since $D_{\ell_j} \leqslant \kappa(p)\ell_j^2 p$. Hence by Dirichlet's theorem on primes in arithmetic progressions we find that the number of $D < X$ obtained in this way is $\gg_p \pi(\sqrt{X})$. □

Proof of Corollary 2. Iwasawa [I] proved that if there is only one prime lying above p in $\mathbb{Q}(\sqrt{D})$ and $p \nmid h(D)$, then p cannot divide the class number of any field in the Iwasawa tower. Since $p|D$ for the relevant discriminants in Theorem 1, it follows that p is ramified and the condition above is satisfied. □

Acknowledgements

The author thanks L. Washington for bringing several new references to his attention, and he thanks the referee for making suggestions which improved the presentation in the paper.

References

[Ca] Carlitz, L.: Arithmetic properties of generalized Bernoulli numbers, *J. reine. angew. Math.* **202** (1959), 174–182.

[C] Cohen, H.: Sums involving the values at negative integers of L-functions of quadratic characters, *Math. Ann.* **217** (1975), 271–285.

[C–L] Cohen, H. and Lenstra, H. W.: Heuristics on class groups of number fields, *Number Theory, (Noordwijkerhout 1983)*, Lecture Notes in Math. 1068, Springer, New York, 1984, pp. 33–62.

[D–H] Davenport, H. and Heilbronn, H.: On the density of discriminants of cubic fields II, *Proc. Roy. Soc. Lond. A* **322** (1971), 405–420.

[F-T] Fukuda, T. and Taya, H.: The Iwasawa λ-invariants of $\mathbb{Z}_p$ extensions of real quadratic fields, *Acta. Arith.* **69** (1995), 277–292.

[G] Greenberg, R.: On the Iwasawa invariants of totally real number fields, *Amer. J. Math.* **98** (1976), 263–284.

[Ha] Hartung, P.: Proof of the existence of infinitely many imaginary quadratic fields whose class number is not divisible by 3, *J. Number Theory* **6** (1974), 276–278.

[Ho1] Horie, K.: A note on basic Iwasawa λ-invariants quadratic fields, *Invent. Math.* **88** (1987), 31–38.

[Ho2] Horie, K.: Trace formulae and imaginary quadratic fields, *Math. Ann.* **288** (1990), 605–612.

[Ho-N] Horie, K. and Nakagawa, J.: Elliptic curves with no rational points, *Proc. Amer. Math. Soc.* **104** (1988), 20–24.

[Ho–On] Horie, K. and Onishi, Y.: The existence of certain infinite families of imaginary quadratic fields, *J. Reine ange. Math.* **390** (1988), 97–133.

[Ic-Su] Ichimura, H. and Sumida, H.: On the Iwasawa invariants of certain real abelian fields, II *Internat. J. Math.* **7** (1996), 721–744.

[I] Iwasawa, K.: A note on class numbers of algebraic number fields, *Abh. Math. Sem. Univ. Hamburg* **20** (1956), 257–258.

[J] Jochnowitz, N.: Congruences between modular forms of half integral weights and implications for class numbers and elliptic curves, Preprint.

[Ko] Koblitz, N.: *Introduction to the Theory of Elliptic Curves and Modular Forms*, Springer-Verlag, New York, 1984.

[Koh-O] Kohnen, W. and Ono, K.: Indivisibility of class numbers of imaginary quadratic fields and orders of Tate-Shafarevich groups of elliptic curves with complex multiplication, *Invent. Math*. **135** (1999), 387–398.

[K-S] Kraft, J. and Schoof, R.: Computing Iwasawa modules of real quadratic number fields, *Compositio Math.* **97** (1995), 135–155.

[M] Murty, M. R.: Private Communication.

[O-Sk] Ono, K. and Skinner, C.: Fourier coefficients of half-integral weight modular forms modulo ℓ, *Ann. Math.* **147**(2) (1998), 451–468.

[Sh] Shimura, G.: On modular forms of half-integral weight, *Ann. Math*. **97** (1973), 440–481.

[St] Sturm, J.: On the congruence of modular forms, In *Lecture Notes in Math*. 1240, Springer, New York, 1984, pp. 275–280.

[W] Washington, L.: *Introduction to Cyclotomic Fields*, Springer-Verlag, New York, 1982.