PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 123, Number 3, March 1995

ON THE EXPONENT OF THE IDEAL CLASS GROUP OF $\mathbf{Q}(\sqrt{-d})$

FRANCESCO PAPPALARDI

(Communicated by Dennis A. Hejhal)

ABSTRACT. Let $m(d)$ be the exponent of the ideal class group of $\mathbf{Q}(\sqrt{-d})$, we establish the bound $m(d) \gg \frac{\log d}{\log\log d}$ for almost all the discriminants d by using uniform asymptotic formulas on the number of $n \leq x$ for which there exists a prime less than s for which n is a quadratic residue.

1. INTRODUCTION

Let d be a positive square-free integer and let $m(d)$ denote the exponent of the class group of $\mathbf{Q}(\sqrt{-d})$, i.e., $m(d)$ is the least positive integer m, such that $x^m = 1$ for every x in the class group.

In 1972 D.W. Boyd and H. Kisilevsky (see [2]) proved that if the Extended Riemann Hypothesis holds, then for any $\eta > 0$ and d sufficiently large,

$$m(d) > \frac{\log d}{(2+\eta)\log\log d} \tag{1.1}$$

which of course implies that $m(d) \to \infty$ as $d \to \infty$.

The goal of this note is to establish unconditional inequalities of the type (1.1) for density-one sets of values of d. Before doing this, let us review the method used by Boyd and Kisilevsky to prove (1.1).

First they noticed that if α is an integer of $\mathbf{Q}(\sqrt{-d})$ which is not in $\mathbf{Z}$, then $N(\alpha) \geq d/4$ and that if p is a rational prime that splits in $\mathbf{Q}(\sqrt{-d})$ and ϖ is a prime ideal above p, then $\varpi^{m(d)}$ is a principal ideal (α); thus,

$$N(\varpi)^{m(d)} = p^{m(d)} = N(\alpha)^{m(d)} \geq (d/4)^{m(d)}.$$

In conclusion,

$$\left(\frac{-d}{p}\right) = 1 \quad \Longrightarrow \quad p \geq (d/4)^{1/m(d)}. \tag{1.2}$$

Then they proved that

Received by the editors May 22, 1993.
1991 *Mathematics Subject Classification*. Primary 11R29; Secondary 11N37.
Key words and phrases. Complex quadratic fields, ideal class group, least prime quadratic residue.
Supported by Consiglio Nazionale delle Ricerche.

If the Extended Riemann Hypothesis holds, then, for any integer d, there exists a prime less than $\log^{2+\eta} d$ *for which $-d$ is a quadratic residue* and this gives (1.1).

Now, let us take $p = 3$ and ask how often is a square-free d a quadratic residue (mod 3)? This happens when $d \equiv 1 \bmod 3$, and the density of such d's is certainly positive

For a positive proportion of square-free integers d,

$$m(d) \geq \frac{\log d/4}{\log 3}.$$

In general we will be able to prove that

Theorem 1.1. *For any $d < x$ there exists a prime $< \log d$ for which $-d$ is a quadratic residue with at the most $O\left(x^{1-A(\log\log x)^{-1}}\right)$ exceptions.*

This is a consequence of Theorem 2.1 below and by (1.2) implies

Theorem 1.2. *For all discriminants $d < x$, we have that*

$$m(d) > \frac{\log d/4}{\log\log d}$$

with at most $O\left(x^{1-A(\log\log x)^{-1}}\right)$ exceptions.

2. The result

Let $\rho(p)$ be any function of p with values in $\{\pm 1\}$. For any integer n, define

$$\mathcal{M}_\rho(n) = \min\left\{p \;\middle|\; p \text{ is prime and } \left(\frac{n}{p}\right) = \rho(p)\right\}.$$

For example $\mathcal{M}_1(n)$ is the least prime for which n is quadratic residue and $\mathcal{M}_\rho(-n) = \mathcal{M}_{\left(\frac{-1}{\cdot}\right)\rho}(n)$.

Let $K_1(x, s)$ (respectively, $K_2(x, s)$) be the set of numbers (respectively, square-free numbers) n up to x such that $\mathcal{M}_\rho(n) > s$. We have that

Theorem 2.1. *Let $k_1(x, s) = |K_1(x, s)|$ and $k_2(x, s) = |K_2(x, s)|$. Then*

$$\text{(a)} \quad k_1(x, s) = \frac{x}{2^{\pi(s)}} \prod_{p \leq s}\left(1 + \frac{1}{p} - \frac{2}{p^2}\right) + O\left(\frac{e^{\theta(s)}\log^3 s}{2^{\pi(s)}}\right);$$

$$\text{(b)} \quad k_2(x, s) = \frac{6}{\pi^2}\frac{x}{2^{\pi(s)}} \prod_{p \leq s}\left(1 + \frac{1}{p+1}\right) + O\left(\frac{x^{1/2}e^{\theta(s)}}{2^{\pi(s)}\log s}\right)$$

uniformly with respect to s (where as usual $\pi(s)$ and $\theta(s)$ are respectively the number of primes up to s and the sum of the logarithms of the primes up to s).

Proof. Let us define P to be the product of all primes up to s. We will start by proving (b).

(b) In order for a square-free number $n \leq x$ to be in $K_2(x, s)$, one must have $\left(\frac{n}{p}\right) = 0$ or $-\rho(p)$ for all primes p up to s. For any divisor Q of P, let A_Q be the set of $n \in K_2(x, s)$ such that

$$\left(\frac{n}{p}\right) = 0 \text{ for any } p \mid Q \quad \text{and} \quad \left(\frac{n}{p}\right) = -\rho(p) \text{ for any } p \,\Big|\, \frac{P}{Q}.$$

Clearly

$$K_2(x, s) = \biguplus_{Q \mid P} A_Q \tag{2.1}$$

where the union is disjoint. Note also that

(2.2)

$$\begin{aligned}|A_Q| &= \#\left\{n \le \frac{x}{Q} \,\Big|\, (n, Q) = 1, n \text{ square-free}, \left(\frac{n}{p}\right) = -\left(\frac{Q}{p}\right) \text{ for any } p \,\Big|\, \frac{P}{Q}\right\} \\ &= \sum{}^{*} \#\left\{n \le \frac{x}{Q} \mid (n, Q) = 1, n \text{ square-free}, \right. \\ &\qquad\qquad \left. n \equiv g_i (\mathrm{mod}\ q_i),\ i = 1, \dots, t\right\}\end{aligned}$$

where we have put $\frac{P}{Q} = q_1 \cdots q_t$ and $\sum{}^{*}$ means that the sum is extended to all the t-tuples $(g_1, \dots, g_t)$, g_i being a congruence class mod q_i such that $\left(\frac{g_i}{q_i}\right) = -\rho(q_i)\left(\frac{Q}{q_i}\right)$.

By the Chinese Remainder Theorem, for each t-tuple $(g_1, \dots, g_t)$, there exists a unique congruence class $M = M(g_1, \dots, g_t)$ $(\mathrm{mod} \frac{P}{Q})$ such that

$$n \equiv g_i \ (\mathrm{mod}\ q_i), \forall i = 1, \dots, t \quad \Longleftrightarrow \quad n \equiv M \left(\mathrm{mod} \frac{P}{Q}\right).$$

Therefore (2.2) equals

$$\sum{}^{*} \#\left\{n \le \frac{x}{Q} \,\Big|\, (n, Q) = 1, n \text{ square-free}, n \equiv M \left(\mathrm{mod} \frac{P}{Q}\right)\right\}. \tag{2.3}$$

Now we need the following two lemmas:

Lemma 2.2. *Let R_1, R_2, R_3 be positive integers with $(R_1, R_3) = (R_2, R_3) = 1$, and define*

$$B_{R_1, R_2, R_3}(y) = \#\{n \le y \mid (n, R_1) = 1,\ n \equiv R_2 \ (\mathrm{mod} R_3)\}.$$

Then, uniformly with respect to $R_1, R_2, R_3 < y$, we have

$$B_{R_1, R_2, R_3}(y) = y \frac{\varphi(R_1)}{R_1 R_3} + O(\vartheta(R_1)),$$

where $\vartheta(R_1)$ is the number of square-free divisors of R_1.

Lemma 2.3. *Let Q_1, Q_2, Q_3 be positive integers with $(Q_1, Q_2) = (Q_2, Q_3) = 1$, and define*

$$C_{Q_1, Q_2, Q_3}(z) = \#\{n \le z \mid n \text{ square-free},\ (n, Q_1) = 1,\ n \equiv Q_3 \ (\mathrm{mod} Q_2)\}.$$

Then, uniformly with respect to $Q_1, Q_2, Q_3 < z$, *we have*

$$C_{Q_1,Q_2,Q_3}(z) = \frac{6}{\pi^2} z \frac{\varphi(Q_1)}{Q_1 Q_2} \prod_{p|Q_1Q_2} \left(1 - \frac{1}{p^2}\right)^{-1} + O\left(z^{1/2}\vartheta(Q_1)\right).$$

Lemmas 2.2 and 2.3 are due, respectively, to Cohen (see [3]) and to Landau (see pp. 633–636 of [6]). Their version is slightly less general, though the proof is similar. One might think that a stronger version of Lemma 2.2, say valid on a range of R_1 of the same order of the range given by the Brun's Sieve, would yield a better error term in Theorem 2.1. On the contrary, it will become clear how this is not influential to the main goal of our discussion.

Proof of Lemma 2.2. We have that

$$\begin{aligned} B_{R_1,R_2,R_3}(y) &= \sum_{d|R_1} \mu(d)\#\{n \le y \mid d|n, \text{ and } n \equiv R_2 \ (\mathrm{mod} R_3)\} \\ &= \sum_{d|R_1} \mu(d)\#\left\{n \le \frac{y}{d} \mid n \equiv R_2 d^* \ (\mathrm{mod} R_3)\right\} = \sum_{d|R_1} \mu(d) \left[\frac{y}{dR_3}\right] \end{aligned}$$

where d^* is the unique congruence class mod R_3 defined by $dd^* \equiv 1 \bmod R_3$ (such a class exists since we have assumed that $(R_1, R_3) =$ and $d|R_3$). Finally

$$B_{R_1,R_2,R_3}(y) = \sum_{d|R_1} \mu(d) \left(\frac{y}{dR_3} + O(1)\right) = y\frac{\varphi(R_1)}{R_1 R_3} + O(\vartheta(R_1)). \quad \square$$

Proof of Lemma 2.3. This is based on the identity

$$\mu^2(n) = \sum_{d^2|n} \mu(d).$$

We have that

$$\begin{aligned} C_{Q_1,Q_2,Q_3}(z) &= \sum_{\substack{n\le z \\ (n,Q_1)=1 \\ n\equiv Q_3 \ (\mathrm{mod} Q_2)}} \mu^2(n) = \sum_{\substack{d^2\delta\le z \\ (d,Q_1)=(\delta,Q_1)=1 \\ d^2\delta\equiv Q_3 \ (\mathrm{mod} Q_2)}} \mu(d) \\ &= \sum_{\substack{d\le z^{1/2} \\ (d,Q_1)=(d,Q_2)=1}} \mu(d) \sum_{\substack{\delta\le \frac{z}{d^2} \\ (\delta,Q_1)=1 \\ \delta\equiv Q_3 d^{*2} \ (\mathrm{mod} Q_2)}} 1 \\ &= \sum_{\substack{d\le z^{1/2} \\ (d,Q_1)=(d,Q_2)=1}} \mu(d) B_{Q_1,Q_3d^{*2},Q_2}(z/d^2) \end{aligned}$$

where the condition $(Q_2, Q_3) = 1$ implies $(d, Q_2) = 1$ and d^* has the same meaning as in the proof of Lemma 2.2. Now apply Lemma 2.2 and get that

(2.4) equals

$$\sum_{\substack{d\le z^{1/2}\\ (d,Q_1Q_2)=1}} \mu(d)\left(\frac{z}{d^2}\frac{\varphi(Q_1)}{Q_1Q_2}+O(\vartheta(Q_1))\right)$$

$$=\frac{z\varphi(Q_1)}{Q_1Q_2}\sum_{\substack{d=1\\ (d,Q_1Q_2)=1}}^{\infty}\frac{\mu(d)}{d^2}+O\left(\sum_{d>z^{1/2}}\frac{z\varphi(Q_1)}{d^2Q_1Q_2}\right)+O\left(z^{1/2}\vartheta(Q_1)\right)$$

and since clearly $\frac{\varphi(Q_1)}{Q_1}<\vartheta(Q_1)$ and

$$\sum_{\substack{d=1\\ (d,Q_1Q_2)=1}}^{\infty}\frac{\mu(d)}{d^2}=\frac{6}{\pi^2}\prod_{p\mid Q_1Q_2}\left(1-\frac{1}{p^2}\right)^{-1},$$

the claim is deduced. □

Now we can apply Lemma 2.3 to (2.2) with $Q_1=Q$, $Q_2=P/Q$, $Q_3=M$, and $z=x/Q$. Note that the number of summands in (2.3) is $\varphi(\frac{P}{Q})/\vartheta(\frac{P}{Q})$; therefore,

$$\begin{aligned}|A_Q|&=\frac{\varphi(\frac{P}{Q})}{\vartheta(\frac{P}{Q})}\left\{\frac{6}{\pi^2}\frac{x}{Q}\frac{\varphi(Q)}{P}\prod_{p\mid P}\left(1-\frac{1}{p^2}\right)^{-1}+O\left(\left(\frac{x}{Q}\right)^{1/2}\vartheta(Q)\right)\right\}\\ &=\frac{6}{\pi^2}\frac{x}{2^{\pi(s)}}\prod_{p\mid P}\left(1+\frac{1}{p}\right)^{-1}\frac{\vartheta(Q)}{Q}+O\left(\frac{x^{1/2}}{2^{\pi(s)}}\frac{\vartheta^2(Q)}{Q^{1/2}\varphi(Q)}\frac{e^{\theta(s)}}{\log s}\right),\end{aligned}\tag{2.4}$$

where we just noticed that $\vartheta(P)=2^{\pi(s)}$ and $\varphi(P)\ll\frac{e^{\theta(s)}}{\log s}$. Now use (2.1) and get

(2.5)

$$\begin{aligned}k_2(x,s)&=\sum_{Q\mid P}|A_Q|\\ &=\frac{6}{\pi^2}\frac{x}{2^{\pi(s)}}\prod_{p\mid P}\left(1+\frac{1}{p}\right)^{-1}\sum_{Q\mid P}\frac{\vartheta(Q)}{Q}+O\left(\frac{x^{1/2}}{2^{\pi(s)}}\frac{e^{\theta(s)}}{\log s}\sum_{Q\mid P}\frac{\vartheta^2(Q)}{Q^{1/2}\varphi(Q)}\right)\\ &=\frac{6}{\pi^2}\frac{x}{2^{\pi(s)}}\prod_{p\mid P}\left(1+\frac{1}{p}\right)^{-1}\prod_{p\mid P}\left(1+\frac{2}{p}\right)+O\left(\frac{x^{1/2}}{2^{\pi(s)}}\frac{e^{\theta(s)}}{\log s}\right).\end{aligned}$$

The last identity follows since $\sum_{Q\mid P}\frac{\vartheta^2(Q)}{Q^{1/2}\varphi(Q)}$ converges as $s\to\infty$. This concludes the proof of (b).

(a) This is simpler than (b). For any $Q\mid P$, define A_Q to be the set of $n\in K_1(x,s)$ such that

$$\left(\frac{n}{p}\right)=0\text{ for any }p\mid Q\quad\text{and}\quad\left(\frac{n}{p}\right)=-\rho(p)\text{ for any }p\,\Big|\,\frac{P}{Q}.$$

Again

$$k_1(x, s) = \sum_{Q|P} |A_Q|, \tag{2.6}$$

and now

$$\begin{aligned} |A_Q| &= \sum^{*} \# \left\{ n \le \frac{x}{Q} \mid n \equiv g_i \ (\mathrm{mod} q_i), \, i = 1, \dots, t \right\} \\ &= \sum {}^{*}\# \left\{ n \le \frac{x}{Q} \,\middle|\, n \equiv M \ (\mathrm{mod} \frac{P}{Q}) \right\} \end{aligned}$$

where the g_i, $i = 1, \dots, t$ and $M = M(g_1, \dots, g_t)$ are defined as above. Now apply Lemma 2.2 with $R_1 = Q$, $R_2 = M$, $R_3 = P/Q$, and $y = \frac{x}{Q}$ and get

$$|A_Q| = \frac{\varphi(\frac{P}{Q})}{\vartheta(\frac{P}{Q})} \left\{ \frac{x}{Q} \frac{\varphi(Q)}{P} + O(\vartheta(Q)) \right\} = 2^{-\pi(s)} \left(x \frac{\varphi(P)}{P} \frac{\vartheta(Q)}{Q} + O\left(\frac{e^{\theta(s)}}{\log s} \frac{\vartheta^2(Q)}{\varphi(Q)} \right) \right).$$

Finally by (2.6),

$$\begin{aligned} k_1(x, s) &= 2^{-\pi(s)} \left(x \prod_{p \le s} \left(1 - \frac{1}{p}\right) \left(1 + \frac{2}{p}\right) + O\left(\frac{e^{\theta(s)}}{\log s} \prod_{p \le s} \left(1 + \frac{4}{p-1}\right) \right) \right) \\ &= 2^{-\pi(s)} \left(x \prod_{p \le s} \left(1 + \frac{1}{p} - \frac{2}{p^2}\right) + O\left(e^{\theta(s)} \log^3 s\right) \right) \end{aligned}$$

which is the claim of (a). □

Note that if we let $k_0(x, s)$ be the number of primes $l \le x$ for which $\mathscr{M}_\rho(l) > s$, then by the same method of Theorem 2.1 and by the Bombieri-Vinogradov Theorem (see [1]) one can prove that uniformly for $s \ll \log x$,

$$k_0(x, s) \sim \frac{\pi(x)}{2^{\pi(s)}}.$$

Proof of Theorem 1.1. We want to estimate

$$\# \{ d \le x \mid \mathscr{M}(d) > \log d \} \tag{2.7}$$

where we write $\mathscr{M}(d)$ for $\mathscr{M}_\rho(d)$ with $\rho(p) = \left(\frac{-1}{p}\right)$. Note that, since the contribution for $d < x^{1/2}$ is $O(x^{1/2})$, we have that (2.7) equals

$$\begin{aligned} &\# \left\{ d : x^{1/2} \le d \le x \mid \mathscr{M}(d) > \log d \right\} + O(x^{1/2}) \\ &\le \# \left\{ d \le x \mid \mathscr{M}(d) > \frac{1}{2} \log x \right\} + O(x^{1/2}). \end{aligned} \tag{2.8}$$

Now apply Theorem 2.1(a) with $s = \frac{1}{2} \log x$ and get that (2.8) is $\ll$; then

$$\begin{aligned} &2^{-\pi(\frac{1}{2} \log x)} \left(x \log\log x + e^{\theta(\frac{1}{2} \log x))} (\log\log x)^3 \right) \\ &\ll x \exp(-A \log x / \log\log x) \end{aligned}$$

where we took $A < \frac{1}{2} \log 2$, say, and this proves the claim. □

3. Conclusions

Although in Theorem 1.1 we consider discriminants of imaginary quadratic fields which are by definition squarefree numbers, statement (b) of Theorem 2.1 does not give anything more than statement (a). This is due to the fact that the set of square-free numbers has nonzero density.

Theorem 2.1(b) can be improved using a version of Lemma 2.3 in which the error term depends on Q_2. The last has been obtained by K. Prachar in [7] for the case $Q_1 = 1$, and his proof can adapted to show the following:

Lemma 3.1. *With the same notation of Lemma 2.3 we have that, uniformly with respect to the parameters,*

$$C_{Q_1,Q_2,Q_3}(z) = \frac{6}{\pi^2} z \frac{\varphi(Q_1)}{Q_1 Q_2} \prod_{p|Q_1Q_2} \left(1 - \frac{1}{p^2}\right)^{-1} + O\left(\frac{z^{1/2}}{Q_2^{1/4}}\left(\vartheta(Q_1) + \frac{\vartheta(Q_2)}{Q_2^{1/2}}\right) + \vartheta(Q_2) Q_2^{1/2}\right).$$

Corollary 3.2. *With the same notation as above, we have that*

$$k_2(x, s) = \frac{6}{\pi^2}\frac{x}{2^{\pi(s)}} \prod_{p\le s}\left(1 + \frac{1}{p+1}\right) + O\left(\left(\frac{x^{1/2}}{2^{\pi(s)} e^{\theta(s)/4}} + e^{\theta(s)/2}\right)\frac{e^{\theta(s)}}{\log s}\right).$$

Proof. It is similar to the proof of Theorem 1.1(b), but in this case we have

$$|A_Q| = \frac{6}{\pi^2}\frac{x}{2^{\pi(s)}}\prod_{p|P}\left(1+\frac{1}{p}\right)^{-1}\frac{\vartheta(Q)}{Q} + O\left(\left(\frac{x^{1/2}}{Q^{1/2}}\frac{Q^{1/4}}{P^{1/4}}\left(\vartheta(Q) + \frac{\vartheta(P)Q^{1/2}}{\vartheta(Q)P^{1/2}}\right) + \frac{P^{1/2}\vartheta(P)}{Q^{1/2}\vartheta(Q)}\right)\frac{\vartheta(Q)}{2^{\pi(s)}\varphi(Q)}\frac{e^{\theta(s)}}{\log s}\right)$$

and therefore

$$\begin{aligned} k_2(x, s) = \sum_{Q|P}|A_Q| &= \frac{6}{\pi^2}\frac{x}{2^{\pi(s)}}\prod_{p\le s}\left(1+\frac{1}{p+1}\right) + \\ &\quad + O\left(\left(\frac{x^{1/2}}{P^{1/4}}\left(\sum_{Q|P}\frac{\vartheta^2(Q)}{Q^{1/2-1/4}\varphi(Q)} + \frac{\vartheta(P)}{P^{1/2}}\sum_{Q|P}\frac{Q^{1/4}}{\varphi(Q)}\right)\right.\right. \\ &\qquad \left.\left. + P^{1/2}\vartheta(P)\sum_{Q|P}\frac{1}{Q^{1/2}\varphi(Q)}\right)\frac{e^{\theta(s)}}{2^{\pi(s)}\log s}\right) \\ &= \frac{6}{\pi^2}\frac{x}{2^{\pi(s)}}\prod_{p\le s}\left(1+\frac{1}{p+1}\right) + O\left(\left(\frac{x^{1/2}}{e^{\theta(s)/4}} + e^{\theta(s)/2}2^{\pi(s)}\right)\frac{e^{\theta(s)}}{2^{\pi(s)}\log s}\right). \end{aligned}$$

The last identity, because both the series $\sum_{Q|P}\frac{1}{Q^{1/2}\varphi(Q)}$ and $\sum_{Q|P}\frac{\vartheta^2(Q)}{Q^{1/2-1/4}\varphi(Q)}$ converge as $s\to\infty$ and $\frac{\vartheta(P)}{P^{1/2}}\sum_{Q|P}\frac{Q^{1/4}}{\varphi(Q)}$, is $o(1)$. $\square$

A general form of Theorem 1.1 can also be proved.

Theorem 3.3. *Let $k_m(x, s)$ be the number of m-free numbers n up to x for which $\mathcal{M}_p(n) > s$. Then, uniformly with respect to s and $m < \sqrt{s}$,*

$$k_m(x, s) = \frac{1}{\zeta(m)}\frac{x}{2^{\pi(s)}}\prod_{p\le s}\left(1-\frac{1}{p^m}\right)^{-1}\left(1+\frac{1}{p}-\frac{2}{p^2}\right) + O\left(\left\{\frac{x^{1/m}}{e^{\theta(s)/m^2}} + e^{\theta(s)/m}m^{\pi(s)}\right\}\frac{e^{\theta(s)}}{2^{\pi(s)}\log s}\right),$$

where $\zeta(s)$ is the Riemann zeta function.

The proof is similar to the one of Theorem 1.1 and uses an m-free version of Lemma 3.1 that is also in [7]. The results of Prachar have been improved by Hooley in [4], making possible another small improvement of Theorem 2.1.

It may be asked whether the approach of Boyd and Kisilevsky can be extended to other classes of fields. If K is Galois over $\mathbf{Q}$ with discriminant d_K, then the condition $\left(\frac{-d}{p}\right) = 1$ in $\mathbf{Q}(\sqrt{-d})$ is analogous to the condition that p splits completely in $K/\mathbf{Q}$. It has been proven by Lagarias, Montgomery, and Odlyzko in [5] that, assuming the Generalized Riemann Hypothesis, the least such p is $\ll (\log d_K)^2$. The second ingredient of Boyd and Kisilevsky's approach is the inequality

$$N(\alpha) \gg d_K$$

for all $\alpha \in O_K\backslash\mathbf{Z}$. In any field with infinitely many units (i.e., not quadratic imaginary), such an inequality is violated infinitely often. Therefore, no direct extension of this method seems immediate.

Finally we point out that the large sieve implies that

$$k_1(x, s) \ll \frac{x+s^2}{s/\log^2 s}.$$

Therefore, if $s = s(x)$ is any function tending to infinity as $x\to\infty$, such that $s(x) = O(\sqrt{x})$, then for all but $O(x\log^2 s/s)$ discriminants $d \le x$, we have

$$e(d) \ge \frac{\log d}{\log s(x)}. \tag{3.1}$$

The bound in (3.1) is worse than the one in Theorem 1.2 but holds for a larger range of s.

Acknowledgments

The author thanks Professor Ram Murty for his indispensable suggestions on how to accomplish these results and Professor Hershy Kisilevsky for a number of interesting observations.

He is also grateful to the referee for a number of corrections and suggestions.

References

1. E. Bombieri, *Le grande crible dans la théorie analytique des nombres*, Astérisque **18** (1974), 201–225.
2. D. W. Boyd and H. Kisilevsky, *On the exponent of the ideal class groups of complex quadratic fields*, Proc. Amer. Math. Soc. **31** (1972), 433–436.
3. E. Cohen, *Remark on a set of integers*, Acta Sci. Math. (Szeged) **25** (1964), 179–180.
4. C. Hooley, *A note on square-free numbers in arithmetic progressions*, Bull. London Math. Soc. **7** (1975), 133–138.
5. J. C. Lagarias, H. L. Montgomery, and A. M. Odlyzko, *A bound for the least prime ideal in the Chebotarev density theorem*, Invent. Math. **54** (1979), 271–296.
6. E. Landau, *Primzahlen*, Chelsea, New York, 1953.
7. K. Prachar, *Über die kleinste quadratfreie Zahl einer arithmetischen Reihe*, Monatsh. Math. **62** (1958), 173–176.

Department of Mathematics and Statistics, McGill University, 805 Sherbrooke Street West, Montreal, Quebec, Canada H3A 2K6

Current address: Dipartimento di Matematica, Terza Università degli studi, Via C. Segre, 2/4, 00146, Roma, Italia

E-mail address: pappa@mat.uniroma3.it