PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 31, No. 2, February 1972

ON THE EXPONENT OF THE IDEAL CLASS GROUPS OF COMPLEX QUADRATIC FIELDS

DAVID W. BOYD[1] AND H. KISILEVSKY

ABSTRACT. Let $m(d)$ denote the exponent of the ideal class group of the complex quadratic field $Q(\sqrt{d})$, where $d<0$ is a fundamental discriminant. It is shown that there are only finitely many d for which $m(d)=3$. Assuming the extended Riemann Hypothesis, it is shown that $m(d)\to\infty$ as $|d|\to\infty$.

If F is the complex quadratic number field $Q(\sqrt{d})$, where $d<0$ is a fundamental discriminant, denote by $C(d)$ the ideal class group of F. Let $m(d)$ be the exponent of the abelian group $C(d)$, i.e. $m(d)$ is the least positive integer m, such that $x^m=1$ for every $x\in C(d)$. Iwasawa has posed the problem of determining $M=\liminf_{|d|\to\infty} m(d)$ so that M is a positive integer or $M=+\infty$. Chowla [3] has shown that there are only finitely many complex quadratic fields with ideal class groups having exactly one class per genus, i.e. there are finitely many complex quadratic fields $Q(\sqrt{d})$, for which $m(d)\leqq 2$. In [6], Shanks conjectures that there are finitely many complex quadratic fields $Q(\sqrt{d})$, for which $m(d)=3$. In this paper we point out the connection between this problem and that of estimating the least prime quadratic residue modulo d. This enables us to establish Shanks' conjecture, and to show under the extended Riemann Hypothesis, that $\liminf_{|d|\to\infty} m(d)=+\infty$.

Let $F=Q(\sqrt{d})$, where $d<0$, and either $d=-d_1$ with d_1 squarefree and $\equiv -1 \pmod 4$, or else $d=-4d_1$ with d_1 squarefree and $\equiv 1, 2 \pmod 4$. Then, if $\mathfrak{O}$ is the ring of algebraic integers of F, we have $\mathfrak{O}=Z+Z\omega$, where $\omega=(-d_1)^{1/2}$ or $\omega=\frac{1}{2}(1+(-d_1)^{1/2})$ according as $d\equiv 0 \pmod 4$ or $d\equiv 1 \pmod 4$.

LEMMA 1. *If* $\alpha\in\mathfrak{O}$, $\alpha\notin Z$, *then* $\alpha\bar{\alpha}=N(\alpha)\geqq|d|/4$.

PROOF. If $d\equiv 0 \pmod 4$, then $d=-4d_1$ and we must have $\alpha=a+b(-d_1)^{1/2}$, where $a, b\in Z$, $b\neq 0$. Hence

$$N(\alpha) = a^2 + b^2 d_1 \geqq d_1 = |d|/4.$$

Received by the editors April 6, 1971.
AMS 1969 *subject classifications*. Primary 1250; Secondary 1041.
Key words and phrases. Complex quadratic field, ideal class group, least prime quadratic residue, extended Riemann Hypothesis.
[1] Supported in part by NSF grant GP 14133.

If $d\equiv 1 \pmod 4$, then $d=-d_1$, and in this case $\alpha=a+b\omega$, where a, $b\in Z$, $b\neq 0$. Thus

$$N(\alpha) = \tfrac{1}{4}[(2a+b)^2 + b^2 d_1] \geqq |d|/4.$$

LEMMA 2. *Let p be a positive rational prime. If $(d/p)=1$, then, $p\geqq(|d|/4)^{1/m(d)}$.*

PROOF. Let p be a rational prime such that $(d/p)=1$. Then the prime p splits in F, i.e. the principal ideal $p\mathfrak{O}=\mathfrak{p}_1\mathfrak{p}_2$, where $\mathfrak{p}_1$, $\mathfrak{p}_2$ are distinct non-zero prime ideals of $\mathfrak{O}$. Since $m(d)$ is the exponent of the ideal class group of F, it follows that $\mathfrak{p}_1^{m(d)}=\alpha\mathfrak{O}$, for some $\alpha\in\mathfrak{O}$, $\alpha\notin Z$. Therefore $p^{m(d)}=N(\alpha)\geqq|d|/4$, so that $p\geqq(|d|/4)^{1/m(d)}$.

THEOREM 1. *If d is a prime, then the least prime quadratic residue modulo d is $O(d^{1/4+\varepsilon})$.*

PROOF. This result is due to A. I. Vinogradov and Ju. V. Linnik [7].

THEOREM 2. *There are only finitely many complex quadratic fields for which $m(d)=3$.*

PROOF. If $F=Q(\sqrt{d})$ is a field for which $m(d)=3$, it follows that $C(d)$ is an elementary abelian 3-group. Therefore, the class number of F must be odd and hence $-d$ must be a prime. By Lemma 2, if $\chi(p)=1$, then $p\geqq(|d|/4)^{1/3}$. Applying Theorem 1, we see that this cannot occur for arbitrarily large $|d|$.

Let $\chi(n)=(d/n)$, so that χ is a real, nonprincipal character modulo $|d|$ (see [2, p. 347]).

In the following we use the extended Riemann Hypothesis in the following form: If χ is a real character, then for $\mathrm{Re}(s)>0$, $L(s,\chi)=0$ only when $\mathrm{Re}(s)=\frac{1}{2}$.

THEOREM 3. *Let $\eta>0$. Assume the extended Riemann Hypothesis. If χ is a real nonprincipal character modulo $|d|$, then for sufficiently large $|d|$, there is a prime p such that $\chi(p)=1$ and $p<(\log|d|)^{2+\eta}$.*

PROOF. We use a number of results from the paper of Littlewood [4]. Let δ, $\varepsilon>0$, and suppose $\chi(p)\neq 1$ for $p<y^{1+3\delta}$, where as in [4] $y=(\log|d|)^{2(1+4\varepsilon)}$. Let $y=v^{-1-2\delta}$, and $\Lambda_1(n)=\Lambda(n)/\log n$. Equation (7.3) of [4], states that

$$\log L(1,\chi) = \sum_{n=1}^{\infty} \frac{\Lambda_1(n)\chi(n)}{n} e^{-nv} + O(A(\varepsilon)y^{1/2-\varepsilon}\log|d|) + O(y^{1/8}).$$

We can estimate the first term as follows, as $|d|\to\infty$,

$$\sum_{n\geqq y^{1+3\delta}} \frac{\Lambda_1(n)\chi(n)}{n} e^{-nv} \leqq \sum_{n\geqq y^{1+3\delta}} \frac{e^{-nv}}{n} = o(1)$$

and

$$\sum_{n<v^{1+3\delta}} \frac{\Lambda_1(n)\chi(n)}{n} e^{-ny}$$

$$= \sum_{p^m<v^{1+\delta}} \frac{\Lambda_1(p^m)\chi(p^m)}{p^m} e^{-p^m y} + \sum_{v^{1+\delta}\leqq p<v^{1+3\delta}} \frac{\chi(p)}{p} e^{-py} + o(1)$$

$$\leqq \sum_{p^m<v^{1+\delta}} \frac{\Lambda_1(p^m)\chi(p^m)}{p^m}(1 + O(v^{-\delta})) + o(1)$$

$$= \sum_{p^m<v^{1+\delta};p\nmid d} (-1)^m \frac{\Lambda_1(p^m)}{p^m} + o(1)$$

$$= \sum_{p^m<v;p\nmid d} (-1)^m \frac{\Lambda_1(p^m)}{p^m} - \sum_{v\leqq p<v^{1+\delta}} \frac{1}{p} + \sum_{v\leqq p<v^{1+\delta};p\mid d} \frac{1}{p} + o(1)$$

$$= -\sum_{p^m<v;p\nmid d} (-1)^{m-1} \frac{\Lambda_1(p^m)}{p^m} - \log(1 + \delta) + o(1).$$

Therefore

$$\log L(1, \chi) \leqq -\sum_{p^m<v;p\nmid d} (-1)^{m-1} \frac{\Lambda_1(p^m)}{p^m} - \log(1 + \delta) + o(1).$$

However, this contradicts the inequality

$$\log L(1, \chi) > -\sum_{p^m<v;p\nmid d} (-1)^{m-1} \frac{\Lambda_1(p^m)}{p^m} + o(1)$$

obtained from (9.5) of [4] by noticing that $S_p=0$ for $p|d$.

THEOREM 4. *Under the extended Riemann Hypothesis, for any* $\eta>0$,

$$m(d) > \{\log |d|\}/\{(2 + \eta)\log\log |d|\},$$

for sufficiently large $|d|$.

PROOF. Let $\eta'=\eta/2$. By Theorem 3, we see that there is a prime p, such that $\chi(p)=1$ and $p<(\log |d|)^{2+\eta'}$, for sufficiently large $|d|$. Applying Lemma 2, we find that $p\geqq(|d|/4)^{1/m(d)}$. Hence $(2+\eta')\log\log |d|>(1/m(d))\log(|d|/4)$ and so $m(d)>\{\log|d|\}/\{(2+\eta)\log\log |d|\}$ for sufficiently large $|d|$.

REMARK. It follows from the work of Ankeny [1] and Montgomery [5], that the least prime quadratic residue modulo d is $O(\log^2|d|)$, under the extended Riemann Hypothesis.

We are grateful to Professor P. T. Bateman for his proof of Theorem 3, and for helpful suggestions concerning the proof of Theorem 4, which is an improvement of the estimate $m(d)>(\log\log |d|)^{1/3}$, which we had originally obtained by a somewhat different argument.

ADDED IN PROOF. The authors have recently learned that P. Weinberger has independently obtained some similar results.

REFERENCES

1. N. C. Ankeny, *The least quadratic non residue*, Ann. of Math. (2) **55** (1952), 65–72. MR **13**, 538.

2. Z. I. Borevič and I. R. Šafarevič, *Number theory*, "Nauka", Moscow, 1964; English transl., Pure and Appl. Math., vol. 20, Academic Press, New York, 1966. MR **30** #1080; MR **33** #4001.

3. S. Chowla, *An extension of Heilbronn's class number theorem*, Quart. J. Math. **5** (1934), 304–307.

4. J. E. Littlewood, *On the class number of the corpus* $P(\sqrt{-k})$, Proc. London Math. Soc. **27** (1927), 358–372.

5. H. Montgomery, *Topics in multiplicative number theory*, Thesis, Cambridge University, Cambridge, 1971.

6. D. Shanks, *New types of quadratic fields having invariants divisible by three*, J. Number Theory (to appear).

7. A. I. Vinogradov and Ju. V. Linnik, *Hyperelliptic curves and the least prime quadratic residue*, Dokl. Akad. Nauk SSSR **168** (1966), 259–261 = Soviet Math. Dokl. **7** (1966), 612–614. MR **35** #125.

DEPARTMENT OF MATHEMATICS, CALIFORNIA INSTITUTE OF TECHNOLOGY, PASADENA, CALIFORNIA 91109

Current address (D. W. Boyd): Department of Mathematics, University of British Columbia, Vancouver 8, B.C., Canada