CLASS NUMBERS AND QUADRATIC RESIDUES

by S. CHOWLA and J. FRIEDLANDER

(Received 25 November, 1974; revised 15 February, 1975)

1. It has long been known that there is a strong connection between the class numbers of quadratic fields and the distribution of quadratic residues. This connection is exemplified, for instance, by the class number formulae of Dirichlet, which have formed the basis of much of the work on the subject of class numbers.

The purpose of this paper is to discuss some of the features of this interplay, with particular reference to the problem of obtaining upper bounds for $g(p)$ the least prime quadratic residue of a prime p.

2. The results of this section are classical.

Let $p \equiv 3(4)$ be prime and assume that the class number $h(-p) = 1$.

Since $\left(\frac{g(p)}{p}\right) = 1$, $g(p)$ splits in $\mathbb{Q}(\sqrt{-p})$ and hence there is a prime ideal $\mathfrak{g}$ with norm $g(p)$.

Since $h(-p) = 1$, $\mathfrak{g}$ must be generated by an integer $\gamma = \frac{a}{2} + \frac{b}{2}\sqrt{-p}$, $(a, b \in Z)$ with

$$N\gamma = \frac{a^2}{4} + p\frac{b^2}{4} = g(p).$$

Thus $g(p) \geqq \frac{p+1}{4}$.

Hence any upper bound for $g(p)$ which is $< \frac{p+1}{4}$ for all sufficiently large p, gives a solution to the class number one problem.

Conversely, the result of Baker and Stark that $h(-p) = 1 \Rightarrow p \leqq 163$, gives an effective upper bound for $g(p)$. Indeed, if $h(-p) > 1$, then there must be a non-principal prime ideal having norm $q < p^{\frac{1}{2}}$, and $\left(\frac{q}{p}\right) = 1$.

Stronger bounds for $g(p)$ are known. Vinogradov and Linnik [3] gave the bound

$$g(p) \ll p^{\frac{1}{4}+\varepsilon}$$

(with no restriction on p) but their result depends on the Theorem of Siegel and hence is not effective.

3. (A) For primes $p \equiv 1(4)$ an upper bound for $g(p)$ may be given by the following simple argument.

If $p \equiv 1(8)$, $g(p) = 2$.

If $p \equiv 5(8)$ and $p > 5$, then we may write p in the form

$$p = a^2 + b^2,$$

https://doi.org/10.1017/S0017089500002718 Published online by Cambridge University Press

where a has an odd prime factor q. Then

$$\left(\frac{q}{p}\right)=\left(\frac{p}{q}\right)=\left(\frac{a^2+b^2}{q}\right)=\left(\frac{b^2}{q}\right)=1 \quad \text{and} \quad q \leqq \sqrt{p-1}.$$

(B) A similar argument is the following:

Let $4a^2$ be the smallest even square $> p$, and let $\theta = 4a^2-p$. Then $\theta \ll p^{\frac{1}{2}}$ and θ must have an odd prime factor q.

$$\left(\frac{q}{p}\right)=\left(\frac{p}{q}\right)=1 \quad \text{and} \quad q \leqq \theta \ll p^{\frac{1}{2}}.$$

4. For primes of the form $p = m^2+1$, one has the conjecture of S. Chowla that

$$h(p) = 1 \Rightarrow m \leqq 26.$$

For these fields the regulator is relatively small and Siegel's Theorem shows that m is bounded. As in the imaginary case, a sufficiently good (effective) upper bound for $g(p)$ would suffice. (This fact has been discovered independently by Y. Yamamoto.)

In fact, we have,

(C) If $p = m^2+1$ is prime, $m > 2$ and $h(p) = 1$, then $g(p) = \dfrac{m}{2}$.

Proof. Using the argument (A) of section **3**, we have for this case

$$g(p) \leqq \frac{m}{2}.$$

On the other hand, reasoning as in section **2**,

$$g(p) = \left|N\gamma\right| = \tfrac{1}{4}\left|a-b\sqrt{p}\right| \ \left|a+b\sqrt{p}\right|.$$

Now $m+\sqrt{p}$ is the fundamental unit, and has norm -1, so that (cf. p. 146 of [**1**]) by multiplying by an appropriate unit, we may assume that

$$0 < b < \frac{am}{p} = \frac{m}{p}\sqrt{4g(p)+b^2p},$$

whence

$$b < 2m\sqrt{\frac{g(p)}{p}} < 2\sqrt{g(p)}.$$

Thus

$$\begin{aligned} a-b\sqrt{p} &= a-bm-\frac{b}{m+\sqrt{(m^2+1)}} \\ &> 1-\frac{b}{2m} \\ &> 1-\frac{\sqrt{g(p)}}{m}. \end{aligned}$$

https://doi.org/10.1017/S0017089500002718 Published online by Cambridge University Press

Also $a+b\sqrt{p} > 2b\sqrt{p}$, and so,

$$g(p) > \frac{b\sqrt{p}}{2}\left(1-\frac{b}{2m}\right).$$

The assumption $b > 1$ gives

$$g(p) > \sqrt{p}\left(1-\frac{\sqrt{g(p)}}{m}\right) \geqq \sqrt{p}\left(1-\frac{1}{\sqrt{2m}}\right) > \frac{\sqrt{p}}{2}$$

which is impossible, since $g(p) \leqq \frac{m}{2}$. Thus $b = 1$, yielding

$$g(p) > \frac{\sqrt{p}}{2}\left(1-\frac{1}{2m}\right) > \frac{m}{2}-\frac{1}{4}.$$

Since $g(p)$ is an integer $g(p) \geqq \frac{m}{2}$, completing the proof.

REMARK: Our original version of (C) was somewhat weaker and we are grateful to the referee for his suggested improvement.

5. We now return to the argument (B) of section 3 and consider the case where $p \equiv 3(4)$, $p = 4a^2-\theta$, where $4a^2$ is the smallest even square $> p$.

We have $\left(\frac{\theta}{p}\right) = 1$ and, for primes $q \mid \theta$, $\left(\frac{p}{q}\right) = 1$.

Thus

$$q \equiv 1(4) \Rightarrow \left(\frac{q}{p}\right) = 1,$$

and

$$q \equiv 3(4) \Rightarrow \left(\frac{q}{p}\right) = -1.$$

Thus, if $g(p) > \theta$, then all the prime divisors of θ are $\equiv 3(4)$, (and incidentally $\lambda(\theta) = 1$, λ being the Liouville function).

Consider now the polynomial

$$P(n) = 4(a+n)^2-p = 4n^2+8an+\theta.$$

We may apply the above to deduce:

(D) If $g(p) > 4T^2+8aT+\theta$, then $P(n)$ contains only prime factors $\equiv 3(4)$, for $0 \leqq n \leqq T$.

Combining this with the result in 2, we obtain

(E) There is a computable constant c such that, if $h(-p) = 1$, then $P(n)$ has only prime factors $\equiv 3(4)$, for $0 \leqq n \leqq c\sqrt{p}$.

This result suggests a type of problem of which we mention only an example, the difficulty of which already seems formidable.

https://doi.org/10.1017/S0017089500002718 Published online by Cambridge University Press

Let $f(a)$ be the least positive integer x, such that x^2+a has some prime factor $\equiv 1(4)$. What can one say about $f(a)$? A good enough upper bound might lead to an analogous argument for $P(n)$ and thus provide another proof of the class number one result.

It is not even clear whether or not $f(a)$ is bounded. It is easy to choose values of a such that the smallest prime factor $\equiv 1(4)$ is large, but it still may be that $a+1$ is divisible by this prime.

If the polynomial x^2+a is replaced by $x+a$ then the corresponding function is trivially bounded, since $x+a \equiv 0(5)$ for some positive $x \leqq 5$. Partly because of this, partly because of the difficulty in proving it unbounded, and partly because of numerical evidence, we are tempted to conjecture that $f(a)$ is bounded.

6. The result (E) is reminiscent of the old result (Euler–Rabinovitch):

$$(*) \qquad h(-p)=1 \Leftrightarrow x^2+x+\frac{p+1}{4} \text{ is prime for } 0 \leqq x \leqq \frac{p-7}{4}.$$

By substituting $x = 0, 1, 2$ we get $q = \frac{p+1}{4}, q+2, q+6$.

A special case of Schinzel's hypothesis H is:

CONJECTURE: There are infinitely many primes q such that $q+2$, $q+6$ and $4q-1$ are also primes.

Although it seems very likely that this conjecture is true, we mention the following curious byproduct of (*).

(F) The falsity of this prime "quadruples" conjecture implies that there are only finitely many p with $h(-p) = 1$, computability of the former implying computability of the latter.

A result analogous to (*) has recently been given by Hendy [2] for complex quadratic fields of class number 2. The result also has an analogue for fields $\mathbb{Q}(\sqrt{p})$, $p = m^2+1$, $h(p) = 1$.

As in the previous section we consider the polynomial $P(n) = 4n^2+8an+\theta$. Here, however, $p \equiv 1(4)$, so for any odd prime factor q of $P(n)$, we have $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) = 1$. If $P(n)$ is composite, then it will have a prime factor $\leqq \sqrt{P(n)}$ and hence, we have:

(G) Let $p \equiv 1(4)$ and $g(p) > \sqrt{4T^2+8aT+\theta}$. Then $P(n)$ is prime for $0 \leqq n \leqq T$.

Combining this with (C), we get

(H) There is a computable constant c such that if $p = m^2+1$ and $h(p) = 1$, then $P(n)$ is prime for $0 \leqq n \leqq c\sqrt{p}$.

Note added July 1, 1975. The function f, defined in Section **5** seems likely to be unbounded after all, since, as Professor H. M. Stark has pointed out, the boundedness of f would contradict Schinzel's hypothesis H.

Indeed, let m be a positive integer and choose any primes $q_0, q_1, \ldots, q_m$ which are $\equiv 3$ (mod 4) and greater than m^2. By the Chinese Remainder Theorem, there is a positive integer

$b \equiv 1 \pmod 8$ satisfying the congruences $b \equiv -i^2 \pmod{q_i}$ for $0 \leqq i \leqq m$.

Let $Q = 8\prod_{i=0}^{m} q_i$,

$$Q_i = \begin{cases} Q/q_i & \text{if } i \text{ even} \\ Q/2q_i & \text{if } i \text{ odd} \end{cases}$$

and $$b_i = \begin{cases} \dfrac{b+i^2}{q_i} & \text{if } i \text{ even} \\ \dfrac{b+i^2}{2q_i} & \text{if } i \text{ odd} \end{cases}$$

and consider the polynomials

$$F_i(y) = yQ_i + b_i \quad (i = 0, \ldots, m).$$

Clearly Q_i and b_i are integers and

$$F_i(y) \equiv 3 \pmod 4 \quad \text{for all integers } y.$$

Furthermore, letting $F(y) = \prod_{i=0}^{m} F_i(y)$, we have:

LEMMA. (A) *The $F_i(y)$ are irreducible.*
(B) *There is no prime p which divides $F(y)$ for all integers y.*

Proof. Since the F_i are linear, it suffices to prove (B). Since the b_j are odd, $2 \nmid F(y)$. If $p \nmid Q$, and $p \mid (yQ_i + b_i)$, then $p \mid (yq + b + i^2)$. If $p \mid F(y)$ for all y, then for each y, there exists an i such that $i^2 \equiv -(yQ+b) \pmod p$. Thus the Legendre symbol $\left(\dfrac{yQ+b}{p}\right)$ is independent of y, which is impossible since $p \nmid Q$. Considering the case where $p = q_i$, we note that if $j \neq i$, then $q_i \nmid b_j$, for otherwise we would have $q_i \mid (b+j^2)$, $q_i \mid (b+i^2)$ and hence $q_i \mid (i^2 - j^2)$ which would contradict $q_i > m^2$. Thus, if $q_i \mid F(y)$ for all y, then $q_i \mid F_i(y)$ for all y, which is impossible since q_i and Q_i are relatively prime. This completes the proof of the lemma.

From the lemma it follows that, if one assumes hypothesis H, then there is a y_0 for which the $F_i(y_0)$ are all primes. Letting $a = y_0 Q + b$, we have $f(a) > m$.

REFERENCES

1. H. Cohn, *A Second Course in Number Theory* (Wiley, 1962).
2. M. D. Hendy, Prime quadratics associated with complex quadratic fields of class number two, *Proc. American Math. Soc.* **43** (1974), 253–260.

3. A. I. Vinogradov and Y. V. Linnik, Hyperelliptic curves and the least prime quadratic residue, *Doklady* (1966) *Tom* **168**, No. 2, 612–614.

INSTITUTE FOR ADVANCED STUDY
PRINCETON, NJ 08540

MASSACHUSETTS INSTITUTE OF TECHNOLOGY
CAMBRIDGE, MA 02139