ON THE DIVISIBILITY OF THE CLASS NUMBER OF QUADRATIC FIELDS

N. C. ANKENY AND S. CHOWLA

1. Introduction. It is well known that there exist infinitely many quadratic extensions of the rationals each with class number divisible by 2. In fact, if the discriminant of the field contains more than two prime factors, then 2 divides the class number. Max Gut [1] generalized this result to show that there exist infinitely many quadratic imaginary fields each with class number divisible by 3. In this present paper we prove that there exist infinitely many quadratic imaginary fields each with class number divisible by g where g is any given rational integer.

The method extends to yield certain results about quadratic real fields, but these are not as sharp as on quadratic imaginary fields.

2. Theorem. In the following we may assume without loss of generality that g is positive, sufficiently large, and even.

LEMMA 1. *Denote by N the number of square-free integers of the form*

$$3^g - x^2, \text{ where } 2 \mid x, \ 0 < x < (2.3^{g-1})^{1/2}.$$

Then, for g sufficiently large,

$$N \geq \frac{1}{25} 3^{g/2}.$$

Proof. Denote by d the expression

$$d = 3^g - x^2, \tag{1}$$

where

$$2 \mid x, \quad 0 < x < (2 \cdot 3^{g-1})^{1/2}. \tag{2}$$

Received September 28, 1953.

The number of such d is

$$\frac{1}{2}(2\cdot 3^{g-1})^{1/2}+O(1).$$

As $2 \mid x$, none of the d's are divisible by 2. The number of d divisible by 3, and, hence, by 9, is less than

$$\frac{1}{6}(2\cdot 3^{g-1})^{1/2}+O(1).$$

For p an odd prime greater than 3, the number of d divisible by p^2 is less than

$$\frac{1}{2p^2}(2\cdot 3^{g-1})^{1/2}+2.$$

Hence the number of square-free d is

$$N \geq \frac{1}{2}(2\cdot 3^{g-1})^{1/2}-\frac{1}{6}(2\cdot 3^{g-1})^{1/2}+O(1)-\sum_{\substack{p\geq 5\\ p^2<3^g}}\frac{1}{2p^2}(2\cdot 3^{g-1})^{1/2}+2)$$

$$\geq \frac{1}{2}(2\cdot 3^{g-1})^{1/2}\left(1-\frac{1}{3}-\sum_{p\geq 5}\frac{1}{p^2}\right)-2\sum_{p^2<3^g}1+O(1)$$

$$\geq \frac{1}{2}(2\cdot 3^{g-1})^{1/2}\left(1-\frac{1}{3}-\sum_{n=5}\frac{1}{n^2}\right)\pm O\left(\frac{1}{g}3^{g/2}\right),$$

by the prime-number theorem. Hence

$$N \geq \frac{1}{2}(2\cdot 3^{g-1})^{1/2}\left(1-\frac{1}{3}-\frac{1}{4}\right)+O\left(\frac{1}{g}3^{g/2}\right)\geq \frac{1}{25}3^{g/2}.$$

THEOREM 1. *For the square-free integers d which satisfy* (1) *and* (2) *we have $g \mid h$, where h denotes the class number of the field $R(\sqrt{-d}\,)$.*

Proof. Consider the quadratic extension of the rationals $R(\sqrt{-d})$. Since

$$3^g = x^2+d,$$

where x is prime to 3 as d is square free, we see that

$$x^2 + d \equiv O(\text{mod } 3).$$

Hence, by the well-known criterion for the splitting of rational primes in quadratic extensions, $(3) = P_1 P_2$ where (3) denotes the principal ideal generated by 3 in $R(\sqrt{-d})$, and P_1, P_2 are two distinct conjugate prime ideals in $R(\sqrt{-d})$.

Let m be the least positive integer such that P_1^m is a principal ideal in $R(\sqrt{-d})$. If possible let $m < g$, and $P_1^m = (\alpha)$ for some integer $\alpha \in R(\sqrt{-d})$. Since $2 \mid g$, we have $2 \mid x$, and, by (1), $d \equiv 1 \pmod 4$. Then

$$\alpha = u + v\sqrt{-d}$$

for rational integers u and v.

Then

$$(3^m) = P_1^m P_2^m = (u + v\sqrt{-d})(u - v\sqrt{-d}) = (u^2 + v^2 d),$$

or

$$3^m = u^2 + v^2 d. \tag{3}$$

By (1) and (2), we have $d > 3^{g-1}$; but if $m < g$, (3) implies

$$3^{g-1} \geq u^2 + v^2 d,$$

so $v = 0$. But then

$$P_1^m = (u),\ P_2^m = (u), \quad \text{or} \quad P_1^m = P_2^m,\ P_1 = P_2,$$

which is false as P_1, P_2 are two distinct prime ideals in $R(\sqrt{-d})$.

Thus we have shown that $m \geq g$; but as $3^g = x^2 + d$, $m = g$. Hence, there exists in $R(\sqrt{-d})$ a prime ideal P_1 whose gth power but none lower is a principal ideal. This immediately implies $g \mid h$.

3. Application. To show that there exist infinitely many fields each with class number divisible by g, we proceed as follows. Theorem 1 shows that there are at least $(1/25)\ 3^{g/2}$ with class number divisible by g. Let $g^t = g_1$ be such that the class number of none of these fields is divisible by g_1. Then, as before, we find at least $(1/25)\ 3^{g_1/2}$ fields with class number divisible by g_1. These fields must be distinct from the previous fields. Repeating this method we see there exist infinitely many quadratic fields with class number divisible by g.

4. A further result. We shall prove:

THEOREM 2. *If d is square free number of the form $d = n^{2g} + 1$, where $n > 4$, then $g \mid h$, where h is the class number of the field $R(\sqrt{d})$.*

Proof. We need only outline the proof of Theorem 2, as in most aspects it is very similar to the proof of Theorem 1. We first show that

$$(n) = \mathfrak{A}\mathfrak{A}' \text{ in } R(\sqrt{d}),$$

where $\mathfrak{A}$, $\mathfrak{A}'$ are two relatively prime conjugate ideals. We then show that $u^2 - dv^2$ (u, v integers) represents no integer other than 0 and 1 whose absolute value is less than $\sqrt{d}$. This follows from the fact that d is of the form $d = w^2 + 1$. Hence the least power of $\mathfrak{A}$ which is a principal ideal is the gth power. This immediately implies $g \mid h$.

The interest of Theorem 2 is somewhat lessened by the fact that it is unknown at present if there exists an infinite number of square-free numbers of the form $n^{2g} + 1$. Hence we are unable to prove a theorem similar to Theorem 1 with regard to quadratic real extensions of the rationals.

REFERENCE

1. Max Gut, *Kubische Klassenkörper über quadratischimaginären Grundkörpern*, Nieuw Arch. Wiskunde (2) **23** (1951), 185-189.

JOHNS HOPKINS UNIVERSITY,
UNIVERSITY OF COLORADO