JOURNAL OF NUMBER THEORY 5, 237–241 (1973)

Real Quadratic Fields with Class Numbers Divisible by n

P. J. WEINBERGER

Department of Mathematics, University of Michigan, Ann Arbor, Michigan 48104

Communicated by D. J. Lewis

Received April 20, 1971

In this note I prove that the class number of $Q(\sqrt{\Delta(x)})$ is infinitely often divisible by n, where $\Delta(x) = x^{2n} + 4$.

The goal of this note is the following theorem.

THEOREM 1. *For all positive integers n, there are infinitely many real quadratic fields with class numbers divisible by n.*

The corresponding theorem for complex quadratic fields was originally proved by Nagell [1].

Let $\Delta = \Delta(x) = x^{2n} + 4$. Theorem 1 follows immediately from Theorem 2 and Lemma 1. The field of rationals will be denoted with Q.

THEOREM 2. *For infinitely many x, the class number of $Q(\sqrt{\Delta})$ is divisible by n, if n is odd and by $n/2$, if n is even.*

LEMMA 1. *For square-free d, $Q(\sqrt{d}) = Q(\sqrt{\Delta})$ for at most finitely many values of x.*

Proof. The fields are the same only if there is an integer y such that

$$\Delta = x^{2n} + 4 = dy^2,$$

which has only a finite number of solutions (x, y) [2, p. 265].

The proof of Theorem 2 requires two simple lemmas, and knowledge of the fundamental unit of $Q(\sqrt{\Delta})$.

LEMMA 2. *For any odd e there are infinitely many primes p for which $T^e - 4$ is irreducible in $\mathbf{F}_p[T]$.*

Proof. $T^e - 4$ is irreducible over Q. Let $\eta_1, \ldots, \eta_e$ be its roots, $\eta_i = \rho^i 4^{1/e}$ where ρ is a primitive eth root of one. The Galois group of the splitting field consists of the automorphisms determined by

$$\sigma_{ab}(\eta_i) = \rho^{ai+b} 4^{1/e} \qquad \text{with} \qquad 0 \leqslant a, \quad b < e, \quad (a, e) = 1.$$

σ_{11} is a cyclic permutation of order e of the roots. By the Frobenius density theorem there are infinitely many primes p for which the splitting field of $T^e - 4$ over $\mathbf{F}_p$ has its Galois group generated by σ_{11}, and so is of degree e. For these p, $T^e - 4$ is irreducible. Q.E.D.

LEMMA 3. *For integers r, s let $c_i(r, s) = \rho_1{}^i + \rho_2{}^i$, where ρ_1 and ρ_2 are the roots of $T^2 - rT - s = 0$.*

(a) *There are integers f_ν such that*

$$c_i(r, s) = \sum_{\nu=0}^{i/2} f_\nu r^{i-2\nu} s^\nu. \tag{1}$$

When i is odd $f_{(i-1)/2} = i, f_0 = 1$.

(b) *If $r, s > 1$, and $j > 1$, then $c_j(r, s) > r^j$.*

Proof. The binomial theorem shows that the coefficients in (1) are rational, so that $c_i(r, s)$ is a polynomial in r and s with rational coefficients. Part (a) of the lemma now follows from the fact that $c_i(r, s) = rc_{i-1}(r, s) + sc_{i-2}(r, s)$ with $c_0(r, s) = 2$ and $c_1(r, s) = r$.

The second part follows immediately from these facts.

LEMMA 4. *If $x > n$ is prime, and $Q(\sqrt{\Delta}) \neq Q(\sqrt{5})$, then the fundamental unit of $Q(\sqrt{\Delta})$ is*

$$\alpha = (x^n + \sqrt{\Delta})/2.$$

Note that Lemma 1 now implies that the fundamental unit is α for all sufficiently large prime x.

Proof. $N(\alpha) = -1$ and $\alpha > 1$. Let the fundamental unit be $\epsilon > 1$, so that for some odd $j > 0$, $\alpha = \epsilon^j$. Since $\epsilon > 1$ implies $r = \mathrm{Tr}(\epsilon) > 0$, the minimal polynomial of ϵ is

$$T^2 - rT - 1, \qquad r > 0$$

Then

$$x^n = \mathrm{Tr}(\alpha) = \mathrm{Tr}(\epsilon^j) = \rho_1{}^j + \rho_2{}^j = c_j(r, 1),$$

so

$$c_j(r, 1) - x^n = 0. \tag{2}$$

Now from (1) $r \mid c_j(r, 1)$, so $r \mid x^n$. If $r = 1$, then $\epsilon = (1 + \sqrt{5})/2$, which is excluded by the hypotheses. Hence, since x is prime, $r = x^k$ with $1 \leqslant k \leqslant n$. By Lemma 3(b),

$$x^n = c_j(r, 1) \geqslant r^j = x^{jk},$$

so $n \geqslant jk$. Since $x > n$ and prime, it follows that $(j, x) = 1$. Then, since j is odd, Lemma 3(a) gives

$$c_j(r, 1)/r \equiv j \pmod{x};$$

so $(c_j(r, 1)/r, x) = 1$, so that, by (2), $x^{n-k} = 1$, so $n = k$, but then $j = 1$ and $\epsilon = \alpha$. Q.E.D.

Assume that x satisfies the hypotheses of Lemma 4. Let

$$\mathfrak{a} = (x^2, 2 + \sqrt{\Delta}).$$

Since x is odd, and prime to Δ, in the order of discriminant Δ the norm of $\mathfrak{a}$ is x^2. Since x is prime to Δ, there is a one-to-one correspondence between residue classes modulo $\mathfrak{a}$ in the order of discriminant Δ and residue classes modulo $\mathfrak{a}$ in the maximal order of $Q(\sqrt{\Delta})$. Hence,

$$N(\mathfrak{a}) = x^2.$$

This may also be seen by actually calculating an integral basis for $\mathfrak{a}$. Now

$$\begin{aligned}\mathfrak{a}^n &= (x^{2n}, x^{2n-2}(2 + \sqrt{\Delta}),\ldots, (2 + \sqrt{\Delta})^n)\\ &= (2 + \sqrt{\Delta})(\sqrt{\Delta} - 2, x^{2n-2},\ldots, (2 + \sqrt{\Delta})^{n-1}),\end{aligned}$$

so $\mathfrak{a}^n \subseteq (2 + \sqrt{\Delta})$, while $N(\mathfrak{a}^n) = x^{2n} = N((2 + \sqrt{\Delta}))$ so that

$$\mathfrak{a}^n = (2 + \sqrt{\Delta}).$$

The proof of Theorem 2 is concluded by showing that the order of $\mathfrak{a}$ in the ideal class group of $Q(\sqrt{\Delta})$ is, for infinitely many x, n when n is odd, and $n/2$ when n is even. Suppose not, so that $\mathfrak{a}^m = (\beta)$ with $n = mk$, where k is odd or 4. Then, since α is the fundamental unit, for some j

$$\beta^k = \pm(2 + \sqrt{\Delta}) \left(\frac{x^n + \sqrt{\Delta}}{2}\right)^j. \tag{3}$$

The value of j is determined only mod k.

If $k = 4$, then $\beta^k > 0$, so the right side of (3) must be positive. Then $N(\beta^4) = (-1)^{j+1} x^{2n}$, so j is one or minus one, and $N(\beta) = \pm x^{n/2}$. Therefore, with $\sigma = (-1)^{(j-1)/2}$,

$$\beta^4 = (x^{2n} + 2\sigma x^n + 4 + (2 + \sigma x^n)\sqrt{\Delta})/2,$$

which is not rational, so the minimal polynomial of β is $T^2 - rT \pm x^{n/2}$ and

$$x^{2n} + 2\sigma x^n + 4 = \mathrm{Tr}(\beta^4) = c_4(r, \pm x^{n/2}) = r^4 \pm 4x^{n/2}r^2 + 2x^n. \quad (4)$$

If $j = 1$, this implies

$$r^2 = (x^{n/2} \pm 1)^2 + 1,$$

which has no solutions with $x > 1$. If $j = -1$ (4) implies that

$$(r^2 \pm 2x^{n/2})^2 = (x^n - 2)^2 + 4x^n,$$

which is impossible mod 8.

If k is odd, a possible minus sign in (3) can be absorbed into β. Define

$$\frac{Y_i + Z_i\sqrt{\Delta}}{2} = (2 + \sqrt{\Delta})\left(\frac{x^n + \sqrt{\Delta}}{2}\right)^i, \qquad i = 0, 1, \ldots .$$

Then $Y_0 = 4$ and $Z_0 = 2$, so a trivial induction shows that

$$Y_i \equiv 4 \pmod{x^n}, \qquad Z_i \equiv 2 \pmod{x^n}, \qquad i = 0, 1, \ldots .$$

Since $Z_j \neq 0$, β is irrational. Therefore, the minimal polynomial of β is $T^2 - rT \pm x^{2n/k}$, so

$$Y_j = \mathrm{Tr}(\beta^k) = c_k(r, \pm x^{2n/k})$$

and by (1),

$$r^k \equiv Y_j \equiv 4 \pmod{x}. \quad (5)$$

Now let e be the largest odd divisor of n, and x be one of the infinite set of primes given in Lemma 2. Then (5) has no solution, for if $r_0{}^k \equiv 4 \pmod{x}$, then

$$T^k - 4 \equiv (T - r_0)f(T) \pmod{x},$$

so

$$T^e - 4 \equiv (T^{e/k} - r_0)f(T^{e/k}) \pmod{x},$$

which contradicts Lemma 2. Q.E.D.

ACKNOWLEDGMENT

During the preparation of this paper the author learned of recent work by Y. Yamamoto [*Osaka Math. J.* 7 (1970), 57–76] in which Theorem 1 is proved in a different manner and with a different set of discriminants. I also wish to thank A. Schinzel for his helpful comments on the exposition of the proof.

REFERENCES

1. T. NAGELL, *Abh. Math. Seminar Univ. Hamburg* **1** (1922), 140–150.
2. L. J. MORDELL, "Diophantine Equations," Academic Press, New York, 1969.