80. On the Class Number of Imaginary Quadratic Number Fields

By Sige-Nobu KURODA
Department of Mathematics, University of Tokyo

(Comm. by Zyoiti SUETUNA, M.J.A., June 12, 1964)

1. It was proved by Nagel [3] that there exist infinitely many imaginary quadratic number fields each with class number divisible by a given integer. This fact was also proved by Humbert [2] and Ankeny-Chowla [1] independently.[1]

Let n be a given integer greater than 1 and S a set of a finite number of rational primes fixed once for all. In this note we shall prove, by a method analogous to that used in [1] or [2], the following

THEOREM 1. *There exist infinitely many imaginary quadratic number field F's each with the following two properties:*

i) *the class number of F is a multiple of n,*

ii) *if $S \ni p$, then p is ramified in F.*

2. Let m be a square-free negative integer and d be the discriminant of the imaginary quadratic number field $F=Q(\sqrt{m})$. We denote by k the norm of a primitive[2] ambiguous integral ideal of F, which is different from the principal ideal $(\sqrt{m})$. Thus k is equal to 1 or a positive proper square-free divisor of d different from $-m$. We define now the number q as follows. If n is odd, or n is even and $k=1$, q is the smallest prime factor of n. If n is even, not a power of 2, and $k \neq 1$, then q is the half of the smallest odd prime factor of n. Finally if n is a power of 2 and $k \neq 1$, then q is an arbitrary real number greater than one. In any case we have $n > n/q$.

THEOREM 2. *Case* i) *Let* $m \equiv 1 \pmod 4$. *If m is expressible in the form*

$$m=(kb)^2-4\,ka^n, \tag{1}$$

where a (>1) and b (>0) are integers such that

$$-m>4\,ka^{n/q} \quad (\textit{or equivalently } 4\,ka^n-4\,ka^{n/q}>(kb)^2), \tag{2}$$

then the class number of $F=Q(\sqrt{m})$ is a multiple of n.

Case ii) *Let* $m \equiv 2, 3 \pmod 4$. *If m is expressible in the form*

$$m=(kb)^2-ka^n,$$

where a (>2) and b (>0) are integers such that

$$-m>ka^{n/q} \quad (\textit{or equivalently } ka^n-ka^{n/q}>(kb)^2)$$

and a is odd, then the clas number of $F=Q(\sqrt{m})$ is a multiple of n.

---

1) The author wishes to express his hearty thanks to Prof. Leopoldt who has kindly drawn the author's attention to the papers cited in this note.

2) "Primitive" means here "not divisible by a rational integer".

PROOF. Case i) If a and b satisfy (1), then kb is odd. So we put $kb=2b'+1$. Put $\omega=(1+\sqrt{m})/2$. Then (1) is equivalent to

$$N(b'+\omega)=ka^n,$$

where N denotes the norm from F to Q. Let p be a rational prime dividing a, then by (1) and the decomposition law of rational primes in F, we have $p=\mathfrak{p}\mathfrak{p}'$, where $\mathfrak{p}$ and its conjugate $\mathfrak{p}'$ are prime ideals in F different from each other. Let l be a rational prime dividing k, then we have $l=\mathfrak{l}^2$, where $\mathfrak{l}$ is a prime ideal in F. Let

$$(3) \qquad (b'+\omega)=\prod \mathfrak{l}_i \cdot \prod \mathfrak{p}_j^{m_j}$$

be the prime ideal decomposition of the principal ideal $(b'+\omega)$ in F, where $\mathfrak{l}_i$ and $\mathfrak{p}_j$ are prime ideals dividing k and a, respectively. As the ideal $(b'+\omega)$ is primitive, there does not appear any pair of conjugate prime ideals in the above decomposition. We have $N(b'+\omega)=\prod l_i \cdot \prod p_j^{m_j}$, where $l_i=N\mathfrak{l}_i$ and $p_j=N\mathfrak{p}_j$. Let $ka=\prod l_i \cdot \prod p_j^{n_j}$, then we have $m_j=nn_j$. Put $\mathfrak{a}=\prod \mathfrak{p}_j^{n_j}$. If n is odd, then $(\prod \mathfrak{l}_i \cdot \mathfrak{a})^n$ is principal, because $\prod \mathfrak{l}_i \cdot \mathfrak{a}^n$ is principal by (3) and the even power of $\prod \mathfrak{l}_i$ is principal. So the order of the ideal class represented by $\prod \mathfrak{l}_i \cdot \mathfrak{a}$ is a factor of n. So it is odd under the assumption that n is odd. Let c be an odd integer such that $0<c\leq n/q$, and assume that $(\prod \mathfrak{l}_i \cdot \mathfrak{a})^c$ is principal. As c is odd, it follows that $\prod \mathfrak{l}_i \cdot \mathfrak{a}^c$ is principal, so we have

$$(4) \qquad \prod \mathfrak{l}_i \cdot \mathfrak{a}^c=\left(\frac{x+y\sqrt{m}}{2}\right),$$

where x and y are integers not equal to zero, because the left-hand side of (4) is primitive and not ambiguous. Thus we get $ka^c>-m/4$. This contradicts (2). Thus $\prod \mathfrak{l}_i \cdot \mathfrak{a}^c$ is not principal for $c\leq n/q$. As q is the smallest prime factor of n, the order of the ideal class represented by $\prod \mathfrak{l}_i \cdot \mathfrak{a}$ is n. This completes the proof in case n is odd. If n is even and $k=1$, then the proof can be done as above. So let n be even and $k\neq 1$. Then $\mathfrak{a}^n$ belongs to some non-principal ambiguous class because of the assumption on k. Thus if n is a power of 2, the order of the ideal class represented by $\mathfrak{a}$ is $2n$. In the remaining case, as $\mathfrak{a}^{2n}$ is principal and $\mathfrak{a}^n$ is not, it suffices to show that $\mathfrak{a}^c$ is not principal for c less than n/q. This can be done by the same method as above. This completes our proof. The proof of Case ii) is similar.

3. Let S be a set of a finite number of rational primes and k the product of all the elements of S. First we assume that S does not contain 2 so that k is a positive square-free odd integer. Let p be a prime large enough so that p is not contained in S. We denote by $N(p)$ the number of square-free integers of the form: $m=(kb)^2-4kp^n$, where $4kp^n-4kp^{n/q}>(kb)^2$ and kb is odd. For such an m, by Theorem 2, the class number of $F=Q(\sqrt{m})$ is a multiple

of n and every rational prime in S is ramified in F.

LEMMA. $\lim_{p\to\infty} N(p)=\infty$.

PROOF. The number of such m's is at least

$$\left[\frac{(4\,kp^n-4\,kp^{n/q})^{1/2}}{2\,k}\right]-1,$$

where $[x]$ denotes the integral part of x. As k and b are odd, none of the m's is divisible by 2. Let $l \neq p$ be an odd prime less than $(4\,kp^n)^{1/2}$. The number of the m's divisible by l^2 is at most

$$\left[\frac{(4\,kp^n-4\,kp^{n/q})^{1/2}}{kl^2}\right]+1.$$

Finally the number of m's divisible by p, hence by p^2, is at most

$$\left[\frac{(4\,kp^n-4\,kp^{n/q})^{1/2}}{kp}\right]+1.$$

Thus we have

$$N(p)>\frac{(4\,kp^n-4\,kp^{n/q})^{1/2}}{k}\left(\frac{1}{2}-\sum_{(4kp^n)^{1/2}>l>2}\frac{1}{l^2}-\frac{1}{p}\right)-\pi((4\,kp^n)^{1/2}),$$

where $\pi(x)$ denotes the number of primes not exceeding x,

$$>\frac{(4\,kp^n-4\,kp^{n/q})^{1/2}}{k}\left(\frac{1}{2}+1-\frac{\pi^2}{6}+\frac{1}{4}\frac{\pi^2}{6}-\frac{1}{p}\right)-\pi((4\,kp^n)^{1/2})$$

$$>\frac{(4\,kp^n-4\,kp^{n/q})^{1/2}}{k}\left(\frac{3}{2}-\frac{\pi^2}{8}-\frac{1}{p}\right)-\pi((4\,kp^n)^{1/2}).$$

As $n>n/q$, we get our Lemma by the prime number theorem.

Now, if S does not contain 2, our Theorem 1 follows from Theorem 2, Case i) and above Lemma. If S contains 2, then Theorem 1 follows from Theorem 2, Case ii) and a slight modification of above Lemma.

References

[1] N. C. Ankeny and S. Chowla: On the divisibility of the class number of quadratic fields. Pacific J. Math., **5**, 321–324 (1955).

[2] P. Humbert: Sur les nombres de classes de certains corps quadratiques. Comment. Math. Helv., **12**, 233–245 (1939/40), also **13**, 68 (1940/41).

[3] Tr. Nagel: Über die Klassenzahl imaginär-quadratischer Zahlkörper. Abh. Math. Sem. Univ. Hamburg, **1**, 140–150 (1922).