11. *On a Lower Bound for the Class Number of an Imaginary Quadratic Field*

By Ryuji SASAKI
Department of Mathematics, College of Science and Technology,
Nihon University

(Communicated by Shokichi IYANAGA, M. J. A., Jan. 13, 1986)

§1. **Introduction.** Let d be a negative square-free integer and let $K=\boldsymbol{Q}(\sqrt{d})$ be the imaginary quadratic field. We denote by ω the integer $\sqrt{d}$ (resp. $(1/2)(1+\sqrt{d})$) if $d\equiv 2$ or 3 (mod 4) (resp. $d\equiv 1$ (mod 4)), and by Δ_K and h_K the discriminant and the class number of K, respectively. We define the polynomial $P(x)$ by

$$P(x)=\begin{cases} x^2+N(\omega) \\ x^2+x+N(\omega) \end{cases} \quad \text{if } \begin{cases} d\equiv 2, 3 \pmod 4 \\ d\equiv 1 \pmod 4, \end{cases}$$

where N stands for the norm map. Following Prof. T. Ono, we define the natural number p_K by

$$p_K=\max_{0\leqslant a\leqslant|\Delta_K|/4-1}\{\text{the number of prime factors of } P(a)\}$$

when $d\neq -1, -3$ and $p_K=1$ when $d=-1, -3$. Using p_K, Rabinovitch's theorem in [2] can be formulated in the following way:

Theorem.

$$h_K=1\Longleftrightarrow p_K=1.$$

The aim of this note is to prove the following:

Theorem 1.

$$h_K\geqslant p_K.$$

Theorem 2.

$$h_K=2\Longleftrightarrow p_K=2.$$

In his lecture at the Johns Hopkins University in the fall of 1984, T. Ono raised the question to examine if these theorems hold.

During the preparation of this note the author obtained useful suggestions from conversation with Prof. Ono and from his lecture, to whom he would like to express his hearty thanks.

§2. **Proof of Theorem 1.** Let $\mathfrak{a}$ be an ideal in the integer ring $\mathcal{O}_K$ of the imaginary quadratic field $K=\boldsymbol{Q}(\sqrt{d})$. Let a be the smallest positive integer in $\mathfrak{a}$ and c the smallest positive integer such that $b+c\omega$ is contained in $\mathfrak{a}$ for some integer b; then a and c are uniquely determined by $\mathfrak{a}$ and b is uniquely determined, modulo a, by $\mathfrak{a}$. In this case the $\boldsymbol{Z}$-module $[a, b+c\omega]$ generated by a and $b+c\omega$ becomes the ideal $\mathfrak{a}$ and its norm $N\mathfrak{a}$ is given by ac. Since $\mathfrak{a}$ is an ideal, both of a and b are divided by c.

Lemma 1. *Let a and b be integers with $a>0$; then the $\boldsymbol{Z}$-module $[a, b+\omega]$ generated by a and $b+\omega$ becomes an ideal if and only if a divides $N(b+\omega)$. In this case the following hold:*

(1) *If $a=a_1a_2$ then $[a, b+\omega]=[a_1, b+\omega][a_2, b+\omega]$.*

(2) *If $1<a<N(\omega)$ then $[a, b+\omega]$ is not a principal ideal.*

Proof. We shall prove the part (2) only. If $\mathfrak{a}=[a, b+\omega]$ is a principal ideal (α), then there exist integers x and y such that $\alpha=ax+(b+\omega)y$. Since K is imaginary, $N(\alpha)$ is positive; hence $N\mathfrak{a}=a=|N(\alpha)|=N(\alpha)=a(ax^2+\mathrm{Tr}\,(b+\omega)xy+(1/a)N(b+\omega)y^2)$. Thus we get $ax^2+\mathrm{Tr}\,(b+\omega)xy+(1/a)N(b+\omega)y^2=a(x+(1/(2a)\,\mathrm{Tr}\,(b+\omega)y)^2+(1/a)(N(b+\omega)-(1/4)\,\mathrm{Tr}\,(b+\omega)^2)y^2=1$; hence $N(b+\omega)-(1/4)\,\mathrm{Tr}\,(b+\omega)^2=N(\omega)-(1/4)\,\mathrm{Tr}\,(\omega)^2\leqslant a$ when $y\neq 0$ or $a=1$ when $y=0$. Therefore we get $a\geqslant N(\omega)$ or $a=1$. Q.E.D.

Lemma 2. *Let a and b be integers such that $a>0$, $a|N(b+\omega)$ and $N(b+\omega)<N(\omega)^2$. Then the ideal $[a, b+\omega]$ is a principal ideal if and only if $a=1$ or $a=N(b+\omega)$.*

Proof. The "if" part is trivial, so we shall prove the "only if" part. Let $a'=N(b+\omega)/a$; then $aa'=N(b+\omega)<N(\omega)^2$. Hence $1\leqslant a<N(\omega)$ or $1\leqslant a'<N(\omega)$. The first case occurs only when $a=1$ by Lemma 1. Since $[a, b+\omega][a', b+\omega]=[aa', b+\omega]=(b+\omega)$, $[a', b+\omega]$ is also principal. By the same reason as the above, the second case occurs only when $a'=1$, i.e., $a=N(b+\omega)$. Q.E.D.

Now we shall prove Theorem 1. When $d=-1$ or -3, the assertion holds trivially. So we may assume $d\neq -1, -3$. By the definition, p_K is the number of prime factors of $P(b)=N(b+\omega)$ for some b satisfying $0\leqslant b\leqslant(1/4)|\Delta_K|-1$. Let $p_1, \cdots, p_n$ $(n=p_K)$ be the set of prime factors of $P(b)$. We denote by $\mathfrak{p}_i$ the ideal $[p_i, b+\omega]$. Then the ideal classes $(\mathfrak{p}_1), (\mathfrak{p}_1\mathfrak{p}_2), \cdots, (\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_n)$ are mutually distinct. For if $(\mathfrak{p}_1\cdots\mathfrak{p}_i)=(\mathfrak{p}_1\cdots\mathfrak{p}_j)$ with $i<j$, then $(\mathfrak{p}_{i+1}\cdots\mathfrak{p}_j)=([p_{i+1}\cdots p_j, b+\omega])=1$; hence $[p_{i+1}\cdots p_j, b+\omega]$ is a principal ideal. On the other hand it is easily seen that $P(b)\leqslant P((1/4)|\Delta_K|-1)<N(\omega)^2$. This contradicts to the result in Lemma 2. Q.E.D.

§3. Proof of Theorem 2. We shall use the fcllowing well known fact (cf. [1]):

Lemma 3. *Any ideal class of K contains an integral ideal $\mathfrak{a}$ such that $N\mathfrak{a}\leqslant\sqrt{|\Delta_K|/3}$.*

For the completeness, we shall give a proof of Ravinovitch's theorem. Since $h_K\geqslant p_K$, we shall prove the implication $p_K=1\Rightarrow h_K=1$. Suppose $h_K>1$. Let $\mathfrak{p}$ be a non-principal ideal having the smallest norm. Then $\mathfrak{p}$ is a prime ideal and $N\mathfrak{p}$ is a rational prime number. In fact if $\mathfrak{p}=\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_t$ is the decomposition into prime ideals, then some $\mathfrak{p}_i$ is not a principal ideal and $N\mathfrak{p}=N\mathfrak{p}_1\cdots N\mathfrak{p}_t$. Hence, by the property of $\mathfrak{p}$, t must be 1. Since $\mathfrak{p}$ is prime, $N\mathfrak{p}$ must be a prime or the square of a prime. If $N\mathfrak{p}$ is the square of a prime, $\mathfrak{p}$ is principal. Furthermore we can assume $N\mathfrak{p}=p\leqslant\sqrt{|\Delta_K|/3}$. Let $\mathfrak{p}=[p, b+\omega]$ for some integer b such that $0\leqslant b\leqslant p$ and $p|N(b+\omega)$. If $d\neq -1, -3$, then $|\Delta_K|\geqslant 6$ and $b<p\leqslant\sqrt{|\Delta_K|/3}\leqslant|\Delta_K|/4$. By the assumption $p_K=1$, $P(b)=N(b+\omega)$ must be a prime; hence $N(b+\omega)=p$ and $\mathfrak{p}=[p, b+\omega]$ is principal. This is a contradiction. If $d=-1$ or -3, we have $h_K=1$.

Q.E.D.

Our original proof of Theorem 2 was somewhat complicated. Dr. J. B. Svirsky suggested to us a simplified proof, which we shall give here.

By the Ravinovitch's theorem and Theorem 1, it is sufficient to show that $p_K=2$ implies $h_K=2$. Let $\mathfrak{p}$ and $\mathfrak{q}$ be non-principal prime ideals such that $N\mathfrak{p}=p$, $N\mathfrak{q}=q\leqslant\sqrt{|\Delta_K|/3}$. Then p and q are prime numbers since $\mathfrak{p}$ and $\mathfrak{q}$ are not principal. Moreover $\mathfrak{p}\mathfrak{q}$ becomes principal. In fact let $\mathfrak{p}\mathfrak{q}=[a, b+c\omega]$ for some integers a, b and c such that $a, c>0$; $c|a$, $c|b$ and $0\leqslant b<a$. Then $ac=N(\mathfrak{p}\mathfrak{q})=N\mathfrak{p}N\mathfrak{q}=pq$; hence $c=1$ and $a=pq$, i.e., $\mathfrak{p}\mathfrak{q}=[pq, b+\omega]$ and $0\leqslant b<pq\leqslant|\Delta_K|/3$. When $pq\geqslant\mathrm{Tr}\,(b+\omega)$, $2b+\mathrm{Tr}\,(\omega)\leqslant\mathrm{Tr}\,(b+\omega)\leqslant pq\leqslant|\Delta_K|/3$; hence $b\leqslant(1/6)|\Delta_K|-\mathrm{Tr}\,(\omega)/2$. If $|\Delta_K|\geqslant 12-6\mathrm{Tr}\,(\omega)$, then $b\leqslant(1/4)|\Delta_K|-1$. Since $p_K=2$, it follows that $P(b)=pq$; hence $\mathfrak{p}\mathfrak{q}=(b+\omega)$ is principal. If $|\Delta_K|<12-6\mathrm{Tr}\,(\omega)$, then $d=-1, -2$ or -3; hence $h_K=1$. When $pq<\mathrm{Tr}\,(b+\omega)$, the conjugate $(\mathfrak{p}\mathfrak{q})'$ of $\mathfrak{p}\mathfrak{q}$ becomes $[pq, b'+\omega]$, where $b'=pq-\mathrm{Tr}\,(b+\omega)+b$. In this case $pq-\mathrm{Tr}\,(b'+\omega)=\mathrm{Tr}\,(b+\omega)-pq>0$. By the same argument as above, we see that $(\mathfrak{p}\mathfrak{q})'$ is principal; hence $\mathfrak{p}\mathfrak{q}$ is principal. Now we shall show that every ideal class is of order 2. Let $\mathfrak{p}$ be an ideal such that $\mathfrak{p}^2$ is not principal and has the smallest norm. Then $\mathfrak{p}$ is a prime ideal, $N\mathfrak{p}=p$ is a rational prime and $p\leqslant\sqrt{|\Delta_K|/3}$. By the above argument, we see that $\mathfrak{p}^2$ is principal. Now suppose $h_K\geqslant 4$. Let $\mathfrak{p}$ be a non-principal ideal having the smallest norm and $\mathfrak{q}$ a non-principal ideal such that $\mathfrak{q}$ is not equivalent to $\mathfrak{p}$ and has the smallest norm; then $\mathfrak{p}$ and $\mathfrak{q}$ satisfy the condition in the first part of the proof. Therefore $\mathfrak{p}\cdot\mathfrak{q}$ is principal. Since both of $\mathfrak{p}^2$ and $\mathfrak{q}^2$ are principal, $\mathfrak{q}$ is equivalent to $\mathfrak{p}$. This is a contradiction. Q.E.D.

Remark. There are quadratic fields $K=\boldsymbol{Q}(\sqrt{d})$ such that $h_K>p_K$. For example when $d=-21$, $h_K=4$ and $p_K=3$.

In [3], we shall treat also the case of real quadratic fields by the same method.

References

[1] T. Ono: Binary quadratic forms. Lecture at The Johns Hopkins University (1984).

[2] G. Rabinovitch: Eindeutigkeit der Zerlegung in Primzahlfaktoren in quadratischen Zahlkörpern. J. reine angew. Math., **142**, 153–164 (1913).

[3] R. Sasaki: Binary quadratic forms representing many primes. (in preparation).