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 $3 \pmod 4$ (resp. $d\equiv 1 \pmod 4$), and by Δ_K and h_K the discriminant and the class number of K, respectively. We define the polynomial $P(x)$ by

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

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 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 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:*