TOKYO J. MATH.
VOL. 6, NO. 2, 1983

A Note on Hasse's Theorem Concerning the Class Number Formula of Real Quadratic Fields

Noriaki KIMURA

Nihon University

(Communicated by T. Kakita)

Let p be a prime with $p\equiv 1 \pmod 4$ and h the class number of the real quadratic field $Q(\sqrt{p})$. Let $\varepsilon>1$ be a fundamental unit of $Q(\sqrt{p})$. As well-known, the Dirichlet's class number formula is stated in the form

$$\varepsilon^h=\frac{\prod_b \sin\frac{\pi b}{p}}{\prod_a \sin\frac{\pi a}{p}}, \tag{1}$$

where a and b runs over quadratic residues and quadratic non-residues between 0 and $p/2$ respectively. As h is a positive integer, the right-hand side of (1) is a unit in $Q(\sqrt{p})$. So ε^h is written in the form $u+v\sqrt{p}$, $u, v\in\mathbf{Q}$. The explicit formula of u and v is given by H. Hasse. (See [1].) In this paper we shall prove an alternative form of Hasse's theorem, which is slightly simpler in structure.

Let g be a fixed positive quadratic non-residue mod p and let $\boldsymbol{a}=(a_1, \cdots, a_n)$ and $\boldsymbol{b}=(b_1, \cdots, b_n)$ be systems of $n=(p-1)/4$ quadratic residues a_ν and quadratic non-residues b_ν with $0<a_\nu, b_\nu<p/2$. Furthermore let $\boldsymbol{x}=(x_1, \cdots, x_n)$, where $-(g-1)\leqq x_\nu\leqq g-1$ and any x_ν is odd or even, according as g is even or odd, be a solution of the congruence, respectively,

$$\boldsymbol{ax}=a_1x_1+\cdots+a_nx_n\equiv a_\nu \pmod p,$$
$$\boldsymbol{ax}=a_1x_1+\cdots+a_nx_n\equiv b_\nu \pmod p,$$

and

$$\boldsymbol{ax}=a_1x_1+\cdots+a_nx_n\equiv 0 \pmod p.$$

We write

Received May 26, 1982

$$A_\nu = \sum_{ax\equiv a_\nu \pmod p} 1$$

$$B_\nu = \sum_{ax\equiv b_\nu \pmod p} 1$$

and

$$C = \sum_{ax\equiv 0 \pmod p} 1 ,$$

which denotes the number of solutions of $\boldsymbol{ax}\equiv a_\nu \pmod p$, $\boldsymbol{ax}\equiv b_\nu \pmod p$ and $\boldsymbol{ax}\equiv 0 \pmod p$ respectively. For discribing our main theorem we need the following

LEMMA. *A_ν and B_ν do not depend on.*

PROOF. It is enough to prove $A_\nu = A_\mu$, $\nu, \mu, =1, \cdots, n$. For two fixed quadratic residues a_ν, a_μ there exists a quadratic residue $r=r(\nu, \mu)$ such that $a_\mu \equiv ra_\nu \pmod p$. Then for each $i=1, \cdots, n$ there exists one and only one j $(j=1, \cdots, n)$ such that $ra_i \equiv \pm a_j \pmod p$. If $\boldsymbol{x}$ is a solution of $\boldsymbol{ax}\equiv a_\nu \pmod p$, then

$$\begin{aligned} r\boldsymbol{ax} = \sum_i ra_i x_i \equiv \sum_j a_j(\pm x_i) & \pmod p \\ \equiv ra_\nu \equiv a_\mu & \pmod p . \end{aligned}$$

Put $\boldsymbol{x}'=(x_1', \cdots, x_n')$, $x_j' = \pm x_i$, then $\boldsymbol{x}'$ is a solution of $\boldsymbol{ax}\equiv a_\mu \pmod p$. In other words we are able to obtain $\boldsymbol{x}'$ from $\boldsymbol{x}$ if we rearrenge x, taking suitable signs. Therefore we conclude $A_\nu = A_\mu$.

From Lemma it follows that A_ν and B_ν can be written A and B respectively, taking off suffices. Our main theorem is now stated as follow.

THEOREM. *Let*

$$v_g = \frac{1}{2}\left\{\lambda_g + \sum_{k=1}^{[(g+1)/2]} \sum_{s\in I_{2k-1}} \left(\frac{s}{p}\right)\right\} ,$$

where I_k is an open interval $((k-1)p/2g, kp/2g)$, λ_g denotes the number of kg $(1\leqq k \leqq (p-1)/2)$, whose smallest positive residue mod p *is greater then $p/2$, $\left(\frac{s}{p}\right)$ is Legendre symbol, finally $[w]$ is Gauss's symbol for a real number w.*

If $p\equiv 5 \pmod 8$, then $\varepsilon^h = (-1)^{v_g}\{C-(A+B)/2-((A-B)/2)\sqrt{p}\}$.

If $p\equiv 1 \pmod 8$, then $\varepsilon^h = -(-1)^{v_g}\{C-(A+B)/2+((A-B)/2)\sqrt{p}\}$.

PROOF. By Corollary 2 and Lemma 2 of [3], it holds that

$$(2) \qquad \varepsilon^h=-(-1)^{v_g}\prod_r(\theta^{(g-1)r}+\theta^{(g-3)r}+\cdots+\theta^{-(g-3)r}+\theta^{-(g-1)r})^{\left(\frac{2}{p}\right)},$$

where θ is a primitive p-th root of unity and r ranges over the quadratic residues mod p between 0 and $p/2$. The right-hand side of (2) can be written in the form

$$-(-1)^{v_g}\left(C+A\left(\sum_{\nu=1}^n\theta^{a_\nu}+\sum_{\nu=1}^n\theta^{-a_\nu}\right)+B\left(\sum_{\nu=1}^n\theta^{b_\nu}+\sum_{\nu=1}^n\theta^{-b_\nu}\right)\right)^{\left(\frac{2}{p}\right)} .$$

On the other hand, it holds that

$$\sum_{\nu=1}^n\theta^{a_\nu}+\sum_{\nu=1}^n\theta^{-a_\nu}+\sum_{\nu=1}^n\theta^{b_\nu}+\sum_{\nu=1}^n\theta^{-b_\nu}=-1$$

and

$$\sum_{\nu=1}^n\theta^{a_\nu}+\sum_{\nu=1}^n\theta^{-a_\nu}-\left(\sum_{\nu=1}^n\theta^{b_\nu}+\sum_{\nu=1}^n\theta^{-b_\nu}\right)=\sqrt{p} .$$

Therefore we have

$$\varepsilon^h=-(-1)^{v_g}\left(C-\frac{A+B}{2}+\frac{A-B}{2}\sqrt{p}\right)^{\left(\frac{2}{p}\right)} .$$

Together with the fact that $N\varepsilon=-1$ and h is odd, this concludes the proof.

If we take $g=2$ in case $p\equiv 5 \pmod 8$, then we get the result of P. Chowla. (See [2].) As an application of the theorem, we can prove the result of [3], which is a generalization of [2], in the same manner as the paper of P. Chowla.

References

[1] H. HASSE, Vorlesungen über Zahlentheorie, Springer, 1950.

[2] P. CHOWLA, On the class-number of real quadratic fields, J. Reine Angew. Math., **230** (1968), 51-60.

[3] N. KIMURA, On the class number of real quadratic fields $Q(\sqrt{p})$ with $p\equiv 1 \pmod 4$, Tokyo J. Math., vol. **2**, no. 2 (1979), 387-396.

Present Address:
COLLEGE OF INDUSTRIAL TECHNOLOGY
NIHON UNIVERSITY
NARASHINO-SHI, CHIBA 275