TOKYO J. MATH.
VOL. 9, NO. 2, 1986

Quadratic Fields and Factors of Cyclotomic Polynomials

Mitsuhiko HIKITA

Osaka University
(Communicated by Y. Kawada)

Introduction

Let p be an odd prime and put $p^*=(-1)^{(p-1)/2}p$. The decomposition of the p-th cyclotomic polynomial $\Phi_p(X)$ in the quadratic field $\boldsymbol{Q}(\sqrt{p^*})$ has been early investigated in Dirichlet [2] and also in Staudt [9] and Lerch [6], the latter considered the decomposition of $\Phi_{|D|}(X)$ in $\boldsymbol{Q}(\sqrt{D})$ for a quadratic discriminant D. Later, Petersson [7], and recently, Williams [12], [13] have also investigated such a decomposition. Let m be the product of r distinct odd primes p_j $(1\leqq j\leqq r)$. In this paper, we consider the decomposition of $\Phi_m(X)$ in the field generated by all $\sqrt{p_j^*}$ over the field $\boldsymbol{Q}$ of rational numbers. Let $\Psi_m(X)$ be an irreducible factor of this decomposition. We derive the formulas for $\Psi_m(1)$, $\Psi_m(1^{1/4})$ and $\Psi_m(1^{1/8})$. Those formulas and our method are not found in any other paper. Our formulas are useful to obtain various results for quadratic fields. We derive certain congruences for the class numbers of imaginary quadratic fields. Those congruences essentially contain lots of results obtained by Lerch [6], Pitzer [8] and Berndt [1] through various methods different from ours. Also we derive some results concerning the class numbers and the norms of the fundamental units of real quadratic fields.

§1. Notation.

For a quadratic discriminant d, $h(d)$ (respectively $\hat{h}(d)$) denote the wide (resp. narrow) class number of the quadratic field $\boldsymbol{Q}(\sqrt{d})$. For $d>0$, ε_d (>1) denotes the fundamental unit of $\boldsymbol{Q}(\sqrt{d})$, and $\hat{\varepsilon}_d$ (>1) denotes the least totally positive unit of $\boldsymbol{Q}(\sqrt{d})$. For $d<0$, we have $h(d)=\hat{h}(d)$. For $d>0$, we have $h(d)=\hat{h}(d)$, $\varepsilon_d^2=\hat{\varepsilon}_d$ (resp. $2h(d)=\hat{h}(d)$, $\varepsilon_d=\hat{\varepsilon}_d$), if $N(\varepsilon_d)=-1$ (resp. $+1$), where N denotes the absolute norm. Let χ_d denote the Kronecker symbol of $\boldsymbol{Q}(\sqrt{d})$. For a prime q, q^* denotes a

Received May 20, 1985

quadratic prime discriminant divisible by q. If q is odd, then $q^*=(-1)^{(q-1)/2}q$ and $\chi_{q^*}(n)=(n/q)$, (Legendre-Jacobi symbol). If $q=2$, then $q^*=-4$, 8 or -8,

$$\chi_{-4}(n)=\begin{cases}(-1)^{(n-1)/2}\,, & \text{if } n \text{ is odd}\,,\\ 0 \,, & \text{if } n \text{ is even}\,,\end{cases}$$

$$\chi_{8}(n)=\begin{cases}(-1)^{(n^2-1)/8}\,, & \text{if } n \text{ is odd}\,,\\ 0 \,, & \text{if } n \text{ is even}\,,\end{cases}$$

and $\chi_{-8}(n)=\chi_{-4}(n)\chi_8(n)$. Letting q_j $(1\leqq j\leqq t)$ be the primes dividing d, we have the decomposition

$$d=q_1^*\cdots q_t^*\,,$$

and

$$\chi_d(n)=\chi_{q_1^*}(n)\cdots\chi_{q_t^*}(n)\,.$$

We put

$$k(d)=h(d)/2^{t-1}\,,\qquad \hat{k}(d)=\hat{h}(d)/2^{t-1}\,.$$

From the genus theory of the quadratic fields, $\hat{k}(d)$ is a rational integer. If $q_j^*>0$ for every j, then $\hat{k}(d)$ is also a rational integer. (e.g. [3] Chapter 26.8). Let K_d denote the field $\boldsymbol{Q}(\sqrt{q_1^*},\cdots,\sqrt{q_t^*})$. The Galois group $G(K_d/\boldsymbol{Q})$ is abelian of the type $(2,\cdots,2)$, t-tuple. For an element σ of $G(K_d/\boldsymbol{Q})$, we define $\sigma_j=\sigma_{q_j^*}$ by

$$\sigma_j=\begin{cases}1\,, & \text{if } \sqrt{q_j^*}^{\,\sigma}=\sqrt{q_j^*}\,,\\ -1\,, & \text{if } \sqrt{q_j^*}^{\,\sigma}=-\sqrt{q_j^*}\,.\end{cases}$$

The correspondance between σ and $(\sigma_1,\cdots,\sigma_t)$ is bijective. We set

$$\operatorname{sgn}\sigma=\prod_{j=1}^{t}\sigma_j\,,$$

so that $\sqrt{d}^{\,\sigma}=\operatorname{sgn}\sigma\sqrt{d}$. If σ is defined over an extation field of K_d then $\sigma(d)$ denotes the restriction of σ to K_d.

Let m be a squarefree odd rational integer and $m=\prod_{j=1}^{r}p_j$ be the prime decomposition. We define the polynomial $\Psi_m(X)$ by

$$\Psi_m(X)=\overset{+}{\prod_{x_1}}\cdots\overset{+}{\prod_{x_r}}(1-X\zeta_{p_1}^{x_1}\cdots\zeta_{p_r}^{x_r})\,,$$

where $\zeta_n=e^{2\pi i/n}$, and each product $\prod_{x_j}^{+}$ is taken over all $x_j \bmod p_j$ such that $(x_j/p_j)=+1$. We put $m^*=\prod_{j=1}^{r}p_j^*$. $\Psi_m(X)$ is one of the irreducible factors of the m-th cyclotomic polynomial $P_m(X)$ over the field K_{m^*}, and the coefficients of $\Psi_m(X)$ are all integral. We have the decomposition

$$P_m(X)=\prod_{\sigma\in G(K_{m^*}/\boldsymbol{Q})}\Psi_m^\sigma(X)\ ,$$

where we put $F^\sigma(X)=\sum_{n=1}^N \alpha_n^\sigma X^n$, for a polynomial $F(X)=\sum_{n=1}^N \alpha_n X^n$ with coefficients in K_{m^*}. We see

$$\Psi_m^\sigma(X)=\prod_{x_1}^{\sigma_1}\cdots\prod_{x_r}^{\sigma_r}(1-X\zeta_{p_1}^{x_1}\cdots\zeta_{p_r}^{x_r})$$

where each product $\prod_{x_j}^{\sigma_j}$ is taken over all $x_j \bmod p_j$ such that $(x_j/p_j)=\sigma_j$.

For a rational integer n $(\neq 0)$, $r(n)$ denotes the number of primes dividing n. For a quadratic discriminant d and a rational integer $\tilde{d}$ $(\neq 0)$, we define $\phi_d^{\tilde{d}}$ by

$$\phi_d^{\tilde{d}}=\begin{cases}\Bigl(\prod\limits_{\substack{p\mid\tilde{d}/d\\ p\ \mathrm{prime}}}(1-\chi_d(p))\Bigr)/2^{r(\tilde{d})-r(d)}\ , & \text{if}\quad d\mid\tilde{d}\ ,\\ 0 & \text{if}\quad d\nmid\tilde{d}\ ,\end{cases}$$

in particular, $\phi_d^{\pm d}=1$. Clearly the value of $\phi_d^{\tilde{d}}$ is 0 or 1.

In the following, we always put $p_{-1}^*=-4$ and $p_0^*=8$. We have $\boldsymbol{Q}(\zeta_4)=\boldsymbol{Q}(\sqrt{p_{-1}^*})$ and $\boldsymbol{Q}(\zeta_8)=\boldsymbol{Q}(\sqrt{p_{-1}^*}, \sqrt{p_0^*})$. For an element σ of $G(\boldsymbol{Q}(\zeta_8)/\boldsymbol{Q})$, we have $\operatorname{sgn}\sigma(-8)=\sigma_{-1}\sigma_0$.

§ 2. Results.

We state our main results.

THEOREM 1. *Let m be the product of r (>0) distinct odd primes p_j $(1\leqq j\leqq r)$. Put the field $K_f=K_{m^*}(\zeta_{2^f})$ with $f=0$, 2 or 3. Let σ be an element of $G(K_f/\boldsymbol{Q})$. Then we have*

$$\Psi_m^\sigma(\zeta_{2^f}^\sigma)=c_{m,f}\prod_{\substack{d\mid 2^f m\\ d\ \mathrm{q.d.}}}\eta_{d,f}^{-\operatorname{sgn}\sigma'(d)\phi_d^{2^f m}\hat{k}(d)}$$

where d runs over all quadratic discriminants dividing $2^f m$,

$$c_{m,f}=\begin{cases}1 & ,\quad \textit{if}\quad r(2^f m)>1\ ,\\ \sqrt{p_1}\ (>0)\ , & \textit{if}\quad r(2^f m)=1\ ,\quad f=0\ ,\quad m=p_1\ ,\\ \sqrt{2}\ (>0)\ , & \textit{if}\quad f=2\ ,\quad m=1\ ,\\ \sqrt[4]{2}\ (>0)\ , & \textit{if}\quad f=3\ ,\quad m=1\ ,\end{cases}$$

$$\eta_{d,f}=\begin{cases}\hat{\varepsilon}_d^{1/2^\nu}\ (>1)\,, & if\ \ d>0\,,\\ \zeta_{2^\nu+1}\,, & if\ \ d<-4\,,\\ \zeta_{2^\nu+2}\,, & if\ \ d=-4\,,\\ \zeta_{3\cdot 2^\nu+1}\,, & if\ \ d=-3\,,\end{cases}$$

with

$$\nu=\begin{cases}1\,, & if\ \ f=0,2\,,\\ 2\,, & if\ \ f=3\,,\end{cases}$$

and σ' *is the element of* $G(K_f/\boldsymbol{Q})$ *such that*

$$\sigma'_j=\chi_{p_j^*}(2^f m/p_j)\sigma_j\,,\quad for\quad j=\begin{cases}1,\cdots,r\,, & if\ \ f=0\,,\\ -1,1,\cdots,r\,, & if\ \ f=2\,,\\ -1,0,1,\cdots,r\,, & if\ \ f=3\,,\end{cases}$$

with $p_{-1}=p_0=2^f$.

THEOREM 2. *We have*

$$\sum_{\substack{d\mid 2^f m\\ d<-4\\ d\ \mathrm{q.d.}}}\operatorname{sgn}\sigma(d)\phi_d^{2^f m}k(d)+\alpha_1\frac{1}{2}\operatorname{sgn}\sigma(-4)\Big(\chi_{-4}(m)\frac{\varphi(m)}{2^r}+\phi_{-4}^{2^f m}\Big)\phi_{-4}^{2^f}$$
$$+\alpha_2\frac{1}{3}\operatorname{sgn}\sigma(-3)\Big(\chi_{-3}(2^f m/3)2^\nu\frac{\varphi(m)}{2^r}+\phi_{-3}^{2^f m}\Big)$$
$$+\alpha_8(\operatorname{sgn}\sigma(8)\chi_8(m)-1)\frac{\varphi(m)}{2^r}\phi_8^{2^f}+2^{\nu-1}\frac{\varphi(m)}{2^r}\equiv 0 \pmod{2^\nu}$$

where φ *denotes the Euler function, and*

$$\alpha_1=1\ \ if\ \ 4\mid 2^f m\,,\quad =0\ \ otherwise\,,$$
$$\alpha_2=1\ \ if\ \ 3\mid 2^f m\,,\quad =0\ \ otherwise\,,$$
$$\alpha_8=1\ \ if\ \ 8\mid 2^f m\,,\quad =0\ \ otherwise\,.$$

THEOREM 3. *Let* D *be the product of* r *distinct real quadratic prime discriminants* p_j^* $(1\leqq j\leqq r)$, *and* p^* *be a real quadratic prime discriminant different from each* p_j^*. *Then we have*

$$\prod_{\substack{d\mid D\\ d>0\\ d\ \mathrm{q.d.}}}N(\varepsilon_{p^*d})^{\phi_{p^*d}^{p^*D}k(p^*d)}=\begin{cases}-1\,, & if\ \ r=0\,,\\ 1\,, & if\ \ r>0\,.\end{cases}$$

COROLLARY. i) $h(p^*)\equiv 1 \pmod 2$ *and* $N(\varepsilon_{p^*})=-1$.

ii) *If* $(p_j/p)=-1$ *for every* j, *and* $(p_i/p_j)=1$ *for every* $i<j$, *then* $h(p^*D)\equiv 2^r \pmod{2^{r+1}}$ *and* $N(\varepsilon_{p^*D})=-1$.

iii) *If* $(p_j/p)=-1$ *for every* j, *and* $(p_i/p_j)=-1$ *for every* $i<j$, *and* $r\equiv 0 \pmod 2$, *then* $h(p^*D)\equiv 2^r \pmod{2^{r+1}}$ *and* $N(\varepsilon_{p^*D})=-1$.

Let p be an odd prime such that $p\nmid m$. Let L be the field generated over $K_f(\sqrt{p^*})$ by $c_{m,f}$ and $\eta_{d,f}$ for every quadratic discriminant $d\,|\,2^f mp$.

Theorem 4. *Let* $\boldsymbol{p}\,|\,p$ *be a prime ideal in* L, *and* τ *be an ellement of* $G(K_f(\sqrt{p^*})/\boldsymbol{Q})$. *Then we have*

$$\prod_{\substack{d|2^f m\\ d \text{ q.d.}}} \eta_{dp^*,f}^{-\operatorname{sgn}\tau(dp^*)\phi_{dp^*}^{2^f mp}\hat{k}(dp^*)} \equiv c_{m,f}^{(p-1)/2} \prod_{\substack{d|2^f m\\ d \text{ q.d.}}} \eta_{d,f}^{\operatorname{sgn}\tau(d)\phi_d^{2^f m}\hat{k}(d)(1-\chi_d(p)p)/2} \pmod{\boldsymbol{p}}\,.$$

§ 3. Preliminary Lemma.

Let d be a quadratic discriminant. From Dirichlet's class number formula for the quadratic fields (e.g. [4] or [10]), we have

$$\sum_{a \bmod d} \chi_d(a)\log(1-\zeta_{|d|}^a) = -h(d)\log\eta_d$$

where

$$\eta_d=\begin{cases}\hat{\varepsilon}_d\ , & \text{if } d>\ 0\,,\\ -1\,, & \text{if } d<-4\,,\\ i\ , & \text{if } d=-4\,,\\ \zeta_6\ , & \text{if } d=-3\,,\end{cases}$$

and log denotes the principal branch of the logarithm.

Lemma. *Letting* $d\,|\,2^f m$ *be a quadratic discriminant, we have*

$$\sum_{\substack{a \bmod 2^f m\\ (a,2^f m)=1}} \chi_d(a)\log(1-\zeta_{2^f m}^a) = -\{\prod_{\substack{p|2^f m/d\\ p \text{ prime}}} (1-\chi_d(p))\}h(d)\log\eta_d\,.$$

Proof. Let p be a prime such that $p\,|\,2^f m/d$. First, suppose p is odd. Put $m'=m/p$ and $a=pa'+2^f m'x$. If a' and x run over complete reduced systems of residues modulo $2^f m'$ and modulo p, respectively, then a runs over complete reduced system of residues modulo $2^f m$. Therefore

$$\begin{aligned}\sum_{\substack{a \bmod 2^f m\\ (a,2^f m)=1}} \chi_d(a)\log(1-\zeta_{2^f m}^a) &= -\sum_{\substack{a \bmod 2^f m\\ (a,2^f m)=1}} \chi_d(a) \sum_{n=1}^{\infty} \frac{1}{n}\zeta_{2^f m}^a)\\ &= -\sum_{\substack{a' \bmod 2^f m'\\ (a',2^f m')=1}} \sum_{n=1}^{\infty} \frac{\chi_d(pa')}{n}\zeta_{2^f m'}^{a'n} \sum_{\substack{x \bmod p\\ (x,p)=1}} \zeta_p^{nx}\end{aligned}$$

where, noticing

$$\sum_{\substack{x \bmod p \\ (x,p)=1}} \zeta_p^{nx} = \begin{cases} -1\ , & \text{if} \quad p \nmid n\ , \\ p-1\ , & \text{if} \quad p \mid n\ , \end{cases}$$

the rearrangement of the formula continues as follows

$$\begin{aligned} &= -\sum_{\substack{a' \bmod 2^f m' \\ (a',2^f m')=1}} \left(\sum_{n=1}^{\infty} \frac{\chi_d(pa')}{n} \zeta_{2^f m'}^{a'n} (-1) + \sum_{n=1}^{\infty} \frac{\chi_d(pa')}{pn} \zeta_{2^f m}^{pa'n} p \right) \\ &= -(-\chi_d(p)+1) \sum_{\substack{a' \bmod 2^f m' \\ (a',2^f m')=1}} \sum_{n=1}^{\infty} \frac{\chi_d(a')}{n} \zeta_{2^f m'}^{a'n} \\ &= (1-\chi_d(p)) \sum_{\substack{a' \bmod 2^f m' \\ (a',2^f m')=1}} \chi_d(a') \log(1-\zeta_{2^f m'}^{a'})\ , \end{aligned}$$

where every interchange of summation is guaranteed by Abel's continuity theorem (e.g. [11] § 3.71). Second, suppose $p=2$. There are three cases, namely, Case i) $f=2$ and d is odd, Case ii) $f=3$ and d is odd, Case iii) $f=3$ and $d \equiv 4 \pmod 8$. Put $a=2^f a'+mx$ in Case i), ii), and $a=a'+4mx$ in Case iii). Then, by the same manner as in the case of $p \neq 2$, noticing that

$$\text{in Case i), ii),} \quad \sum_{\substack{x \bmod 2^f \\ x \text{ odd}}} \zeta_{2^f m}^{nx} = \begin{cases} -2^{f-1}\ , & \text{if} \quad n \equiv 2^{f-1} \pmod{2^f}\ , \\ 2^f-2^{f-1}\ , & \text{if} \quad n \equiv 0 \pmod{2^f}\ , \\ 0\ , & \text{otherwise}\ , \end{cases}$$

$$\text{in Case iii),} \quad \sum_{x=0}^{1} \zeta_2^{nx} = \begin{cases} 2\ , & \text{if} \quad n \equiv 0 \pmod 2\ , \\ 0\ , & \text{if} \quad n \equiv 1 \pmod 2\ , \end{cases}$$

we obtain

$$\begin{aligned} &\sum_{\substack{a \bmod 2^f m \\ (a,2m)=1}} \chi_d(a) \log(1-\zeta_{2^f m}^{a}) \\ &\quad = \begin{cases} (1-\chi_d(2)) \displaystyle\sum_{\substack{a' \bmod m \\ (a',m)=1}} \chi_d(a') \log(1-\zeta_m^{a'})\ , & \text{in Case i), ii)}\ , \\ (1-\chi_d(2)) \displaystyle\sum_{\substack{a' \bmod 4m \\ (a',2m)=1}} \chi_d(a') \log(1-\zeta_{4m}^{a'})\ , & \text{in Case iii)}\ . \end{cases} \end{aligned}$$

Now, by the induction on $r(2^f m/d)$ and the class number formula, we get the Lemma.

§ 4. Proof of Theorem 1.

We see

$$(1)\qquad \sum_{\substack{a \bmod 2^f m\\(a,2^f m)=1}} \{\prod_{p_j^*|2^f m} (\sigma_j'+\chi_{p_j^*}(a))\}\log(1-\zeta_{2^f m}^a)$$

$$=\kappa \sum_{\substack{d|2^f m\\d=1 \text{ or q.d.}}} \operatorname{sgn}\sigma'(d) \sum_{\substack{a \bmod 2^f m\\(a,2^f m)=1}} \chi_d(a)\log(1-\zeta_{2^f m}^a)\ ,$$

where

$$\kappa=\prod_{p_j^*|2^f m} \sigma_j'\ .$$

Observing

$$\prod_{p_j^*|2^f m} (\sigma_j'+\chi_{p_j^*}(a))=\begin{cases}\kappa 2^{r+\mu}\ , & \text{if } \chi_{p_j^*}(a)=\sigma_j' \text{ for every } p_j^*\,|\,2^f m\ ,\\ 0\ , & \text{otherwise}\ ,\end{cases}$$

with

$$\mu=\begin{cases}0\ , & \text{if } f=0\ ,\\ 1\ , & \text{if } f=2\ ,\\ 2\ , & \text{if } f=3\ ,\end{cases}$$

the left hand side of (1) is equal to

$$(2)\qquad \kappa 2^{r+\mu} \sum{}' \log(1-\zeta_{2^f m}^a)\ ,$$

where the summation $\sum'$ runs over all $a \bmod 2^f m$ such that $\chi_{p_j^*}(a)=\sigma_j'$ for every $p_j'|2^f m$. Put $m_j=m/p_j$ for $j=1, 2, \cdots, r$, and $a=mx_0+\sum_{j=1}^r 2^f m_j x_j$. If x_0 and x_j runs over complete reduced system of residues modulo 2^f and modulo p_j, respectively, then a runs over a complete reduced system of residues modulo $2^f m$. Therefore, since $\chi_{p_j^*}(a)=\sigma_j'$ is equivalent to $\chi_{p_j^*}(x_j)=\sigma_j$, the formula (2) is further equal to

$$(3)\qquad \kappa 2^{r+\mu} \sum_{x_1}^{\sigma_1} \cdots \sum_{x_r}^{\sigma_r} \log(1-\zeta_{2^f}^{\sigma}\zeta_{p_1}^{x_1} \cdots \zeta_{p_r}^{x_r})\ .$$

On the other hand, applying the Lemma, the right hand side of (1) is equal to

$$(4)\qquad -\kappa \sum_{\substack{d|2^f m\\d \text{ q.d.}}} \operatorname{sgn}\sigma'(d)\{\prod_{\substack{p|2^f m\\p \text{ prime}}} (1-\chi_d(p))\}h(d)\log \eta_d+\kappa \log P_{2^f m}(1)\ .$$

The equality between (3) and (4) proves Theorem 1.

§ 5. Proof of Theorem 2.

Let $\alpha\rightarrow\alpha^\rho$ be the complex conjugation. We have

$$\begin{aligned}(\Psi_m^\sigma(\zeta_{2f}^\sigma))^\rho &= \prod_{x_1}^{\sigma_1} \cdots \prod_{x_r}^{\sigma_r} (1-(\zeta_{2f}^\sigma)^{-1}\zeta_{p_1}^{-x_1} \cdots \zeta_{p_r}^{-x_r}) \\ &= \prod_{x_1}^{\sigma_1} \cdots \prod_{x_r}^{\sigma_r} (-1)(\zeta_{2f}^\sigma)^{-1}\zeta_{p_1}^{-x_1} \cdots \zeta_{p_r}^{-x_r}(1-\zeta_{2f}^\sigma\zeta_{p_1}^{x_1} \cdots \zeta_{p_r}^{x_r}) \\ &= (-1)^N(\zeta_{2f}^\sigma)^{-N}\Big(\prod_{x_1}^{\sigma_1} \zeta_{p_1}^{x_1}\Big)^{-N_1} \cdots \Big(\prod_{x_r}^{\sigma_r} \zeta_{p_r}^{x_r}\Big)^{-N_r} \Psi_m^\sigma(\zeta_{2f}^\sigma) ,\end{aligned}$$

where we put $N=\varphi(m)/2^r$ and $N_j=\varphi(m_j)/2^{r-1}$. For an odd prime p (>3), letting g be a primitive root modulo p, we see

$$\sum_{x \text{ mop } p}^{+} x = \sum_{n=0}^{(p-3)/2} g^{2n} = \frac{1-g^{p-1}}{1-g^2} \equiv 0 \quad (\text{mod}\, p) ,$$

so that we have

$$\prod_{x \text{ mod } p}^{+} \zeta_p^x = \begin{cases} 1 , & \text{if} \quad p>3 , \\ \zeta_3 , & \text{if} \quad p=3 , \end{cases}$$

and, similarly

$$\prod_{x \text{ mod } p}^{-} \zeta_p^x = \begin{cases} 1 , & \text{if} \quad p>3 , \\ \zeta_3^{-1} , & \text{if} \quad p=3 . \end{cases}$$

Hence, in view of $\varphi(m)/2^r=\varphi(m/3)/2^{r-1}$ if $3|m$, we get

$$(-1)^N(\zeta_{2f}^\sigma)^{-N}\Big(\prod_{x_1}^{\sigma_1} \zeta_{p_1}^{x_1}\Big)^{-N_1} \cdots \Big(\prod_{x_r}^{\sigma_r} \zeta_{p_r}^{x_r}\Big)^{-N_r} = \begin{cases} (-\zeta_{2f}^\sigma)^{-N} , & \text{if} \quad 3\nmid m , \\ (-\zeta_{2f}^\sigma\zeta_3^\sigma)^{-N} , & \text{if} \quad 3|m . \end{cases}$$

Therefore, as $\arg(\alpha)\equiv(1/2)\arg(\alpha/\alpha^\rho)$ (mod π) where $\arg(\gamma)$ denotes the argment of γ, we obtain

$$(5) \qquad \arg(\Psi_m^\sigma(\zeta_{2f}^\sigma)) \equiv \begin{cases} \dfrac{N}{2}\arg(-\zeta_{2f}^\sigma) \quad (\text{mod}\, \pi) , & \text{if} \quad 3\nmid m , \\ \dfrac{N}{2}\arg(-\zeta_{2f}^\sigma\zeta_3^\sigma) \quad (\text{mod}\, \pi) , & \text{if} \quad 3|m . \end{cases}$$

On the other hand, from Theorem 1, we have

$$(6) \qquad \arg(\Psi_m^\sigma(\zeta_{2f}^\sigma)) \equiv \arg\Big(\prod_{\substack{d|2^f m \\ d<0 \\ d \text{ q.d.}}} \eta_{d,f}^{-\operatorname{sgn} \sigma'(d)\phi_d^{2^f m}\hat{k}(d)} \Big) \quad (\text{mod}\, 2\pi) .$$

From (5) and (6), exchanging σ with σ', it follows that

$$-\frac{1}{2^{\varkappa}}\sum_{\substack{d|2^f m\\ d<-4\\ d\ \text{q.d.}}} \operatorname{sgn}\sigma(d)\phi_d^{2^f m}k(d)-\frac{1}{2^{\nu+1}}\operatorname{sgn}\sigma(-4)\phi_{-4}^{2^f m}-\frac{1}{2^{\nu}3}\operatorname{sgn}\sigma(-3)\phi_{-3}^{2^f m}$$

$$\equiv\begin{cases}\dfrac{N}{2}+\dfrac{N}{2\pi}\arg(\zeta_{2^f}^{\sigma'}) & (\operatorname{mod} 1)\,, \quad \text{if} \quad 3\nmid m\,,\\[2ex] \dfrac{N}{2}+\dfrac{N}{2\pi}\arg(\zeta_{2^f}^{\sigma'}\zeta_3^{\sigma'}) & (\operatorname{mod} 1)\,, \quad \text{if} \quad 3\mid m\,.\end{cases}$$

Here, since $\zeta_{2^f}^{\sigma}=\zeta_{2^f}^{\sigma'_{-1}{}^{+2(\sigma'_0-1)}}$, we see

$$\frac{1}{2\pi}\arg(\zeta_{2^f}^{\sigma'})\equiv\frac{1}{2^{\nu+1}}\operatorname{sgn}\sigma(-4)\chi_{-4}(m)\phi_{-4}^{2^f}+\frac{1}{2^{\nu}}(\operatorname{sgn}\sigma(8)\chi_8(m)-1)\phi_8^{2^f} \quad (\operatorname{mod} 1)\,,$$

and

$$\frac{1}{2\pi}\arg(\zeta_3^{\sigma'})\equiv\frac{1}{3}\operatorname{sgn}\sigma(-3)\chi_{-3}(2^f m/3) \quad (\operatorname{mod} 1)\,, \quad \text{if} \quad 3\mid m\,,$$

which proves Theorem 2.

§ 6. Proof of Theorem 3 and Corollary.

There are three cases, namely, Case i) P^*D is odd, Case ii) $p^*=8$, Case iii) $D\equiv 0 \pmod 8$. In Case i), by Theorem 1, we have

$$\Psi_{pD}^{\sigma}(1)=c_{pD,0}\prod_{d|D}\varepsilon_d^{-\text{sng}\,\sigma'(d)\phi_d^{pD}k(d)}\varepsilon_{pd}^{-\operatorname{sgn}\sigma'(pd)\phi_{pd}^{pD}k(pd)}\,.$$

Applying the conjugation δ_p ($\sqrt{p}\rightarrow-\sqrt{p}$), we get

$$\Psi_{pD}^{\sigma\delta_p}(1)=c_{pD,0}^{\delta_p}\prod_{d|D}\varepsilon_d^{-\operatorname{sgn}\sigma'(d)\phi_d^{pD}k(d)}(\varepsilon_{pd}^{\delta_p})^{-\operatorname{sgn}\sigma'(pd)\phi_{pd}^{pD}k(pd)}\,.$$

Hence we obtain

$$(7)\qquad \Psi_{pD}^{\sigma}(1)\Psi_{pD}^{\sigma\delta_p}(1)=N(c_{pD,0})\prod_{a|D}\varepsilon_d^{-2\operatorname{sgn}\sigma'(d)\phi_d^{pD}k(d)}N(\varepsilon_{pd})^{-\operatorname{sgn}\sigma'(pd)\phi_{pd}^{pD}k(pd)}\,.$$

On the other hand, again by Theorem 1, and since $\operatorname{sgn}(\sigma\delta_p)'(d)=\operatorname{sgn}\sigma'(d)$, $\operatorname{sgn}(\sigma\delta_p)'(pd)=-\operatorname{sgn}\sigma'(pd)$, we get

$$\Psi_{pD}^{\sigma\delta_p}(1)=c_{pD,0}\prod_{d|D}\varepsilon_d^{-\operatorname{sgn}\sigma'(d)\phi_d^{pD}k(d)}\varepsilon^{\operatorname{sgn}\sigma'(pd)\phi_{pd}^{pD}k(pd)}\,,$$

so that we obtain

$$(8)\qquad \Psi_{pD}^{\sigma}(1)\Psi_{pD}^{\sigma\delta_p}(1)=c_{pD,0}^2\prod_{d|D}\varepsilon_d^{-2\operatorname{sgn}\sigma'(d)\phi_d^{pD}k(d)}\,.$$

From (7) and (8), we obtain Theorem 3 in Case i). By Theorem 1, we have

$$\left.\begin{array}{ll}\text{in Case ii),} & c_{D,3}^{2}\Psi_{D}^{\sigma}(\zeta_{8}^{\sigma})\Psi_{D}^{\sigma}((\zeta_{8}^{\sigma})^{-1}) \\ \text{in Case iii),} & \Psi_{pD/8}^{\sigma}(\zeta_{8}^{\sigma})\Psi_{pD/8}^{\sigma}((\zeta_{8}^{\sigma})^{-1})\end{array}\right\} = \prod_{\substack{d|D \\ d>0 \\ d \text{ q.d.}}} \varepsilon_{d}^{-\operatorname{sgn}\sigma(d)\phi_{d}^{p*D}k(d)}\varepsilon_{p*d}^{-\operatorname{sgn}\sigma(p*d)\phi_{p*d}^{p*D}k(p*d)} .$$

Hence, by exactly the same way as in Case i), we obtain Theorem 3 in these cases.

We prove Corollary by induction on r. By Theorem 3, we have

$$(9) \qquad N(\varepsilon_{p*D})^{k(p*D)} = \prod_{\substack{d|D \\ 0<d<D \\ d \text{ q.d.}}} N(\varepsilon_{p*d})^{\phi_{p*d}^{p*D}k(p*d)} .$$

In the Case ii) of Corollary, we have $\phi_{p*d}^{p*D}=1$ for every $d|D$. Hence, by (9) and the induction assumption, we get

$$N(\varepsilon_{p*D})^{k(p*D)} = \prod_{\substack{d|D \\ 0<d<D \\ d \text{ q.d.}}} N(\varepsilon_{p*d})^{k(p*d)} = (-1)^{\sum_{\substack{d|D \\ 0<d<D \\ d \text{ q.d.}}} 1}$$
$$= (-1)^{2^{r}-1} = -1 ,$$

which proves the Case ii) of Corollary. In the Case iii) of Corollary, we have

$$\phi_{p*d}^{p*D} = \begin{cases} 1 , & \text{if} \quad r(d) \text{ odd} , \\ 0 , & \text{if} \quad r(d) \text{ even} , \end{cases}$$

for every $d|D$. Hence, by (9) and the induction assumption, we get

$$N(\varepsilon_{p*D})^{k(p*D)} = \prod_{\substack{d|D \\ 0<d<D \\ d \text{ q.d.} \\ r(d) \text{ even}}} N(\varepsilon_{p*d})^{k(p*d)} = (-1)^{\sum_{\substack{d|D,\ 0<d<D \\ d \text{ q.d.}, r(d) \text{ even}}} 1}$$

where we have

$$\sum_{\substack{d|D \\ 0<d<D \\ d \text{ q.d.} \\ r(d) \text{ even}}} 1 \equiv \sum_{\substack{d|D \\ 0<d<D \\ d \text{ q.d.}}} (r(d)+1) \equiv \sum_{\substack{d|D \\ 0<d<D \\ d \text{ q.d.}}} r(d)+1 \pmod 2$$
$$= \sum_{j=0}^{r-1} \binom{r}{j} j + 1 = r \sum_{j=0}^{r-1} \binom{r-1}{j-1} + 1$$
$$= r(2^{r-1}-1)+1 \equiv \begin{cases} 1 \pmod 2 , & \text{if} \quad r \text{ even or } r=1 , \\ 0 \pmod 2 , & \text{if} \quad r \ (>1) \text{ odd} . \end{cases}$$

This proves the Case iii) of Corollary.

§ 7. Proof of Theorem 4.

Putting $p_{r+1}=p$, and applying Theorem 1 to mp and τ, we get

$$
\begin{aligned}
(10)\qquad & \prod_{x_1}^{\tau_1}\cdots\prod_{x_{r+1}}^{\tau_{r+1}}(1-\zeta_{2^f}^{\tau}\zeta_{p_1}^{x_1}\cdots\zeta_{p_{r+1}}^{x_{r+1}}) \\
&= \prod_{\substack{d|2^f mp \\ d\ \text{q.d.}}} \eta_{d,f}^{-\operatorname{sgn}\tau'(d)\phi_d^{2^f mp}k(d)} \\
&= \Big(\prod_{\substack{d|2^f m \\ d\ \text{q.d.}}} \eta_{d,f}^{-\operatorname{sgn}\tau'(d)\phi_d^{2^f mp}k(d)}\Big)\Big(\prod_{\substack{d|2^f m \\ d\ \text{q.d.}}} \eta_{dp^*,f}^{-\operatorname{sgn}\tau'(dp^*)\phi_{dp^*}^{2^f mp}k(dp^*)}\Big)\ ,
\end{aligned}
$$

where τ' is an element of $G(K_f(\sqrt{p^*})/\boldsymbol{Q})$ such that $\tau'_j=\chi_{p_j^*}(2^f mp/p_j)\tau_j$. Let $\boldsymbol{P}$ be a prime ideal in $L(\zeta_p)$, dividing $\boldsymbol{p}$. Then, putting $\sigma=\tau_{|K_f}$, and since $\zeta_p\equiv 1 \pmod{\boldsymbol{P}}$, the left hand side of (10) is congruent to

$$
\Big(\prod_{x_1}^{\sigma_1}\cdots\prod_{x_r}^{\sigma_r}(1-\zeta_{2^f}^{\tau}\zeta_{p_1}^{x_1}\cdots\zeta_{p_r}^{x_r})\Big)^{(p-1)/2}
$$

modulo $\boldsymbol{p}$, which is, again by Theorem 1, equal to

$$
(11)\qquad c_{m,f}^{(p-1)/2}\prod_{\substack{d|2^f m \\ d\ \text{q.d.}}} \eta_{d,f}^{-\operatorname{sgn}\sigma'(d)\phi_d^{2^f m}k(d)(p-1)/2}\ ,
$$

where σ' is an element of $G(K_f/\boldsymbol{Q})$ such that $\sigma'_j=\chi_{p_j^*}(2^f m/p_j)\sigma_j$. From (10) and (11), it follows that

$$
\begin{aligned}
&\prod_{\substack{d|2^f m \\ d\ \text{q.d.}}} \eta_{dp^*f}^{-\operatorname{sgn}\tau'(dp^*)\phi_{dp^*}^{2^f mp}k(dp^*)} \\
&\qquad \equiv c_{m,f}^{(p-1)/2}\prod_{\substack{d|2^f m \\ d\ \text{q.d.}}} \eta_{d,f}^{-\{\operatorname{sgn}\sigma'(d)\phi_d^{2^f m}((p-1)/2)-\operatorname{sgn}\tau'(d)\phi_d^{2^f mp}\}k(d)} \pmod{\boldsymbol{p}}\ ,
\end{aligned}
$$

where, since $\operatorname{sgn}\sigma'(d)=\operatorname{sgn}\tau'(d)\chi_d(p)$ and $\phi_d^{2^f mp}=\phi_d^{2^f m}(1-\chi_d(p))/2$, we see

$$
\operatorname{sgn}\sigma'(d)\phi_d^{2^f m}\frac{p-1}{2}-\operatorname{sgn}\tau'(d)\phi_d^{2^f mp}=\operatorname{sgn}\tau'(d)\phi_d^{2^f m}\frac{\chi_d(p)p-1}{2}\ ,
$$

which, by exchanging τ' with τ, proves Theorem 4.

§ 8. Some applications.

We derive some special congruences from our results. They are only examples, we can obtain more congruences of these types by the similar way.

Application 1: Let $p\equiv 1$, $q\equiv 3 \pmod 8$ be primes such that $(p/q)=-1$.

Then, by Theorem 2, we have

$$k(-8pq)+k(-pq)+k(-8p)+k(-8q)+k(-q)\equiv 0 \pmod 4\,,$$
$$k(-8p)+k(-4p)\equiv 0 \pmod 4\,,$$

and

$$k(-8q)+k(-q)-\frac{q-3}{4}\equiv 0 \pmod 4\,.$$

It follows that

$$k(-8pq)+k(-pq)+k(-4p)\equiv\frac{q-3}{4} \pmod 4\,.$$

This is the formula (19) of Proposition 5 in Pitzer [8].

Application 2: Let p be a prime such that $p\equiv 3 \pmod 8$, $p\equiv 2$ (mod 3). Then, by Theorem 2, we have

$$k(-24p)+k(-12p)+k(-8p)+\frac{23p-13}{12}\equiv 0 \pmod 4\,.$$

It follows that

$$k(-24p)+3k(-12p)+k(-8p)\equiv\begin{cases}0 \pmod 4\,, & \text{if} \quad p\equiv 11 \pmod{16}\,,\\ 2 \pmod 4\,, & \text{if} \quad p\equiv 3 \pmod{16}\,.\end{cases}$$

This is the third and the forth formula of Corollary 11.6 in Berndt [1].

Application 3: Let $p\equiv 3 \pmod 4$ be a prime. We put $\varepsilon_{4p}=t+u\sqrt{p}$ with rational integers t, u. It is easy to see that $u\equiv 1 \pmod 2$, and $t\equiv 0$ (resp. 2) (mod 4), if $p\equiv 7$ (resp. 3) (mod 8). We put $\omega=1-\zeta_8$. Then $\sqrt{2}=\zeta_8^3\varepsilon_8\omega^2$. Since $(1-\zeta_p^x)(1-i\zeta_p^x)^2\equiv 1+\zeta_p^x+\zeta_p^{2x}+\zeta_p^{3x} \pmod{\omega^6}=(1-\zeta_p^{4x})/(1-\zeta_p^x)$, we get $\Psi_p(1)\Psi_p(i)^2\equiv 1 \pmod{\omega^6}$. Hence, by Theorem 1, it follows that

$$\sqrt{p}\, i^{-h(-p)}\varepsilon_{4p}^{h(4p)}(-1)^{-\phi_{-p}^{4p}h(-p)}i\equiv 1 \pmod{\omega^6}\,.$$

Therefore, as $\varepsilon_{4p}^2=t^2+2tu\sqrt{p}+u^2p\equiv -1 \pmod 4$, we obtain

$$\sqrt{p}\,\varepsilon_{4p}(-1)^{(h(4p)-1)/2}(-1)^{(1-h(-p))/2}\equiv\begin{cases}1 \pmod 4\,, & \text{if} \quad p\equiv 7 \pmod 8\,,\\ -1 \pmod 4\,, & \text{if} \quad p\equiv 3 \pmod 8\,.\end{cases}$$

Here, we see

$$\sqrt{p}\,\varepsilon_{4p}=t\sqrt{p}+up\equiv\begin{cases}-u \pmod{\omega^6}\,, & \text{if} \quad p\equiv 7 \pmod 8\,,\\ u \pmod{\omega^6}\,, & \text{if} \quad p\equiv 3 \pmod 8\,.\end{cases}$$

Thus, in view of $u \equiv (-1)^{(u-1)/2}$ (mod 4), we get

$$(-1)^{(u+1)/2}(-1)^{(h(4p)-h(-p))/2} \equiv 1 \pmod 4 ,$$

which proves

$$h(-p) \equiv h(4p)+u+1 \pmod 4 .$$

This is the result of Williams [12].

Application 4: Let $p \equiv 1$ (mod 4) be a prime. By Theorem 3, we see $N(\varepsilon_{8p}) = -1$, $k(8p) \equiv 1$ (mod 2), if and only if $p \equiv 5$ (mod 8). We put $\varepsilon_{8p} = t+u\sqrt{2p}$ with rational integers t, u. We see $t \equiv u \equiv 1$ (mod 2). By Theorem 1, we have

$$\frac{\Psi_p(\zeta_8)}{\Psi_p(-\zeta_8)} = \varepsilon_{8p}^{-k(8p)} i^{-k(-8p)} \varepsilon_8 i \ . \tag{12}$$

As $\zeta_8^4 = -1$, we set $\Psi_p(\zeta_8) = \sum_{j=0}^{3} \alpha_j \zeta_8^j$ with integers α_j in $\boldsymbol{Q}(\sqrt{p})$. Since $X^{(p-1)/2}\Psi_p(X^{-1}) = \Psi_p(X)$, we have $\zeta_8^{(p-1)/2}\Psi_p(\zeta_8^{-1}) = \Psi_p(\zeta_8)$. Here, comparing the coefficients of ζ_8^j, we get $\alpha_0 = \alpha_2$, $\alpha_3 = 0$, if $p \equiv 5$ (mod 16), and $\alpha_0 = -\alpha_2$, $\alpha_1 = 0$, if $p \equiv 13$ (mod 16). Hence, observing $\zeta_8 + \zeta_8^{-1} = \sqrt{2}$, we may set $\Psi_p(\zeta_8) = \zeta_8^{(p-1)/4}(\alpha+\sqrt{2}\beta)$ with integers α, β in $\boldsymbol{Q}(\sqrt{p})$. Applying the conjugation δ_2 ($\sqrt{2} \to -\sqrt{2}$), we get $\Psi_p(-\zeta_8) = (-\zeta_8)^{(p-1)/4}(\alpha-\sqrt{2}\beta)$. Therefore, as $\alpha+\sqrt{2}\beta \equiv \alpha-\sqrt{2}\beta$ (mod ω^6), we obtain $\Psi_p(\zeta_8)/\Psi_p(-\zeta_8) \equiv -1$ (mod ω^6). Thus, from (12), we get

$$\varepsilon_{8p}^{-k(8p)} i^{-k(-8p)} \varepsilon_8 i \equiv -1 \pmod{\omega^6} . \tag{13}$$

We have $\varepsilon_{8p} \pm \varepsilon_8 = t \pm 1 + 2\sqrt{2}((1+\sqrt{p})/2) \equiv t \pm 1$ (mod ω^6), so that, in view of $\varepsilon_8^2 \equiv -1$ (mod ω^6), we see $\varepsilon_{8p} \equiv (-1)^{(t-1)/2}\varepsilon_8 \equiv \varepsilon_8^t$ (mod ω^6). Hence, by (13), we obtain

$$\varepsilon_8^{-(tk(8p)-1)} i^{-(k(-8p)-1)} \equiv (-1)^{-(tk(8p)-1)/2}(-1)^{-(k(-8p)-1)/2} \equiv -1 \pmod{\omega^6} ,$$

which proves

$$tk(8p)+k(-8p) \equiv 0 \pmod 4 .$$

This is equivalent to the result of Williams [13].

Application 5: Let $p \equiv q \equiv 1$ (mod 4) be primes. By Theorem 3, we see $N(\varepsilon_{8pq}) = -1$, $k(8pq) \equiv 1$ (mod 2), if and only if in either of the following three cases,

i) $p \equiv 1$ (mod 8), $q \equiv 5$ (mod 8), $(p/q) = -1$,

ii) $p \equiv q \equiv 5$ (mod 8), $(p/q) = -1$,

iii) $p \equiv q \equiv 5$ (mod 8), $(p/q) = 1$.

By Theorem 1, we have, respectively,

$$(14)\qquad \frac{\Psi_{pq}(\zeta_8)}{\Psi_{pq}(-\zeta_8)}=\begin{cases}\varepsilon_{8pq}^{-k(8pq)}i^{-k(-8pq)}\varepsilon_{8q}^{k(8q)}i^{k(-8q)}\,, & \text{if}\quad \text{i})\,,\\ \varepsilon_{8pq}^{-k(8pq)}i^{-k(-8pq)}\varepsilon_{8}^{-1}i^{-1}\,, & \text{if}\quad \text{ii})\,,\\ \varepsilon_{8pq}^{-k(8pq)}i^{-k(-8pq)}\varepsilon_{8p}^{k(8p)}i^{k(-8p)}\varepsilon_{8q}^{k(8q)}i^{k(-8q)}\varepsilon_{8}^{-1}i^{-1}\,, & \text{if}\quad \text{iii})\,.\end{cases}$$

Similarly as in Application 4, we see $\Psi_{pq}(\zeta_8)/\Psi_{pq}(-\zeta_8)\equiv 1 \pmod{\omega^6}$ and $\varepsilon_{8pq}\equiv\varepsilon_8^t$, $\varepsilon_{8p}\equiv\varepsilon_8^{t_p}$, $\varepsilon_{8q}\equiv\varepsilon_8^{t_q} \pmod{\omega^6}$, where we put $\varepsilon_{8pq}=t+u\sqrt{2pq}$, $\varepsilon_{8p}=t_p+u_p\sqrt{2p}$ and $\varepsilon_{8p}=t_q+u_q\sqrt{2q}$ with rational integers t, u, t_p, u_p, t_q, u_q. Therefore, from (14), we get

$$(15)\qquad \left.\begin{array}{rl}\text{i)} & \varepsilon_8^{-tk(8pq)}i^{-k(-8pq)}\varepsilon_8^{t_qk(8q)}i^{k(-8q)}\\ \text{ii)} & \varepsilon_8^{-tk(8pq)}i^{-k(-8pq)}\varepsilon_8^{-1}i^{-1}\\ \text{iii)} & \varepsilon_8^{-tk(8pq)}i^{-k(-8pq)}\varepsilon_8^{t_pk(8p)}i^{k(-8p)}\varepsilon_8^{t_qk(8q)}i^{k(-8q)}\varepsilon_8^{-1}i^{-1}\end{array}\right\}\equiv 1 \pmod{\omega^6}\,,$$

where, in view of (13), we have

$$(16)\qquad \varepsilon_8^{t_pk(8p)}i^{k(-8p)}\equiv\varepsilon_8^{t_qk(8q)}i^{k(-8q)}\equiv-\varepsilon_8^{-1}i^{-1} \pmod{\omega^6}\,.$$

From (15) and (16), we obtain

$$tk(8pq)+k(-8pq)\equiv\begin{cases}0 \pmod 4\,, & \text{if}\quad \text{i})\,,\\ 2 \pmod 4\,, & \text{if}\quad \text{ii}),\ \text{iii})\,.\end{cases}$$

This formula for the Cases i) and ii) is the result of Hikita [5].

In [5] the author have simplified and extended the method of Williams [13] to the above Cases i) and ii). The proof in [5] is rather complicated and seems difficult to apply in more general cases.

References

[1] B. C. Berndt, Classical theorems on quadratic residues, Enseign Math., **22** (1976), 261-304.

[2] G. L. Dirichlet, Recherches sur diverses applications de l'analyse infinitésimale à la théorie des nombres, seconde partie, J. Reine Angew. Math., **21** (1840), 134-155.

[3] H. Hasse, "Zahlentheorie" 3. Auflage, Akademie Verlag Berlin, 1969.

[4] E. Hecke, "Vorlesungen über die Theorie der algebraischen Zahlen" 2. Auflage, Akademie Verlag Leipzig, 1954.

[5] M. Hikita, The class numbers of $Q(\sqrt{\pm 2pq})$ modulo 2^4, manuscript unpublished 1983.

[6] M. Lerch, Essais sur le calcul du nombre des classes de formes quadratiques binaires aux coefficients entiers, Acta Math., **30** (1906), 203-293.

[7] H. Petersson, Über eine Zerlegung des Kreisteilungspolynoms von Primzahlordnung, Math. Nachr., **14** (1955), 361-375.

[8] A. Pizer, On the 2-part of the class number of imaginary quadratic number fields, J. Number Theory, **8** (1976), 184-192.

[9] G. K. C. von Staudt, Über die Functionen Y und Z, welche der Gleichung $4(x^p-1)/(x-1)=Y^2\mp pZ^2$ Genüge leisten, wo p eine Primzahl der Form $4k\pm 1$ ist, J. Reine Angew.

Math., **67** (1867), 205–217.

[10] T. TAKAGI, "Shotô-Seisû-Ron-Kôgi" (Lectures on the elementary theory of numbers) (in japanese) second ed., Kyoritu, Tokyo, 1971.

[11] E. T. WHITTAKER and G. N. WATSON, "A Course of Modern Analysis" fourthed., Cambridge Univ. Press, London, 1927.

[12] K. S. WILLIAMS, The class number of $\boldsymbol{Q}(\sqrt{-p})$ modulo 4, for $p \equiv 3 \pmod 4$ a prime, Pacific J. Math., **83** (1979), 565–570.

[13] K. S. WILLIAMS, The class number of $\boldsymbol{Q}(\sqrt{-2p})$ modulo 8, for $p \equiv 5 \pmod 8$ a prime, Rocky Mountain J. Math., **11** (1981), 19–26.

Present Address:
DEPARTMENT OF MATHEMATICS
FACULTY OF SCIENCE
OSAKA UNIVERSITY
3-23-30, TERAIKEDAI
TONDABAYASHI, OSAKA, 584