TOKYO J. MATH.
VOL. 2, NO. 2, 1979

On the Class Number of Real Quadratic Fields $Q(\sqrt{p})$ with $p\equiv 1 \pmod 4$

Noriaki KIMURA

Ashikaga Institute of Technology
(Communicated by H. Sunouchi)

Introduction

Let p be a prime number with $p\equiv 1(\bmod 4)$, and h the class number of the real quadratic field $\boldsymbol{Q}(\sqrt{p})$. Let $\varepsilon=(t+u\sqrt{p})/2$ be the fundamental unit of $\boldsymbol{Q}(\sqrt{p})$ with $\varepsilon>1$. If $p\equiv 5(\bmod 8)$, then P. Chowla has proved (see [1])

$$(-1)^{(h-1)/2}\frac{t}{2}\equiv(-1)^m 2^{(p-1)/4} \pmod p ,$$

and

$$\frac{((p-1)/2)!}{2^{(p-1)/4}}\equiv-(-1)^m \pmod p ,$$

where

$$m=\frac{1}{2}\left\{\frac{p-1}{4}+\sum_{s<p/4}\left(\frac{s}{p}\right)\right\} ,$$

and $\left(\frac{s}{p}\right)$ is Legendre's symbol. We shall prove a generalization of these results.

§1. Notations.

Throughout this paper we shall use the following notations.
p: a prime number with $p\equiv 1 \pmod 4$
$\boldsymbol{Q}$: the rational number field
h: the class number of the real quadratic field $\boldsymbol{Q}(\sqrt{p})$
$\varepsilon=(t+u\sqrt{p})/2$: the fundamental unit of $\boldsymbol{Q}(\sqrt{p})$ with $\varepsilon>1$
$\theta=e^{2\pi i/p}$
$\zeta=e^{\pi i/p}$

Received January 18, 1979

$\theta_x=\theta^x$, $\zeta_x=\zeta^x$, where x is a positive integer
n: any quadratic non-residue mod p between 0 and $p/2$
r: any quadratic residue mod p between 0 and $p/2$
g: any positive quadratic non-residue of p
$\chi(a)=\left(\frac{a}{p}\right)$: Legendre's symbol, where a is an integer
$[w]$: the greatest integer which does not exceed a real number w

§2. Theorems.

In this paper we shall prove the following results.

THEOREM 1.

$$(-1)^{(h-1)/2}\frac{t}{2}\equiv-(-1)^{(p-1)/4+v_g}g^{(p-1)/4}\pmod p,$$

where

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

I_k *is an open interval* $((k-1)p/2g, kp/2g)$, *and* λ_g *denotes the number of multiples* kg*'s* $(1\leqq k\leqq(p-1)/2)$, *whose smallest positive residues* mod p *are greater than* $p/2$.

THEOREM 2.

$$\frac{((p-1)/2)!}{g^{(p-1)/4}}\equiv(-1)^{(p-1)/4+v_g}\pmod p.$$

From the Theorems 1 and 2 we have immediately

THEOREM 3. *If* $p\equiv1(\text{mod }4)$, *then*

$$\left(\frac{p-1}{2}\right)!\equiv(-1)^{(h+1)/2}\frac{t}{2}\pmod p.$$

REMARK. It is stated in [1] that the Theorem 3 will be proved in "Proceedings of the National Academy of Science (U.S.A.)". But we could not find his paper related to this result in it.

REMARK. From our theorems we can easily prove P. Chowla's theorem which is stated in the beginning of this paper. If $p\equiv5(\text{mod }8)$, we can take $g=2$, and

$$\lambda_g=\frac{p-1}{4},\qquad\sum_{k=1}^{[(g+1)/2]}\sum_{s\in I_{2k-1}}\left(\frac{s}{p}\right)=\sum_{0<s<p/4}\left(\frac{s}{p}\right).$$

So

$$v_2=\frac{1}{2}\left\{\frac{p-1}{4}+\sum_{0<s<p/4}\left(\frac{s}{p}\right)\right\}=m .$$

This v_2 is the m in the paper of P. Chowla.

§3. Proof of the Theorem 1.

From the classical formula of Dirichlet, we have

$$(1)\qquad 2h\log\varepsilon=-\frac{\tau_x(\chi)}{\sqrt{p}}\sum_{s=1}^{p-1}\chi(s)\log(1-\theta^{xs}) ,$$

where x is a positive integer with $x\not\equiv 0(\mathrm{mod}\ p)$ and

$$\tau_x(\chi)=\sum_{s=1}^{p-1}\chi(s)\theta^{xs}=\chi(x)\sum_{s=1}^{p-1}\chi(s)\theta^{s}=\chi(x)\sqrt{p}$$

is the Gauss's sum.
From (1)

$$\varepsilon^{2h}=\prod_{s=1}^{p-1}(1-\theta^{xs})^{-\chi(xs)} .$$

Since $\sum_{s=1}^{p-1}s\chi(s)=0$, we have

$$\begin{aligned}\varepsilon^{2h}&=\prod_{s=1}^{p-1}(\zeta_x^{s}-\zeta_x^{-s})^{-\chi(xs)}\\&=\prod_{s=1}^{(p-1)/2}(\zeta_x^{s}-\zeta_x^{-s})^{-\chi(xs)}\prod_{s=(p+1)/2}^{p-1}(\zeta_x^{s}-\zeta_x^{-s})^{-\chi(xs)} .\end{aligned}$$

Put $s'=p-s$, then we have as the second factor

$$\prod_{s=(p+1)/2}^{p-1}(\zeta_x^{s}-\zeta_x^{-s})^{-\chi(xs)}=\prod_{s'=1}^{(p-1)/2}(\zeta_x^{p-s'}-\zeta_x^{-p+s'})^{-\chi(xs')} .$$

Since $\zeta_x^{p-s'}-\zeta_x^{-p+s'}=\pm(\zeta_x^{s'}-\zeta_x^{-s'})$ and $(p-1)/2$ is even, it follows

$$\prod_{s=(p+1)/2}^{p-1}(\zeta_x^{s}-\zeta_x^{-s})^{-\chi(xs)}=\prod_{s'=1}^{(p-1)/2}(\zeta_x^{s'}-\zeta_x^{-s'})^{-\chi(xs')} .$$

Therefore we get

$$\varepsilon^{2h}=\left(\sum_{s=1}^{(p-1)/2}(\zeta_x^{s}-\zeta_x^{-s})^{-\chi(xs)}\right)^2 .$$

So

$$\varepsilon^h = \pm \prod_{s=1}^{(p-1)/2} (\zeta_x^s - \zeta_x^{-s})^{-\chi(xs)}$$
$$= \pm \prod_{s=1}^{(p-1)/2} \left(2i \sin \frac{\pi xs}{p}\right)^{-\chi(xs)}$$
$$= \pm \prod_{s=1}^{(p-1)/2} \left(\sin \frac{\pi xs}{p}\right)^{-\chi(xs)} .$$

We wish to determine the sign here. Since $\varepsilon > 0$, the sign is $(-1)^{m_x}$, where m_x is the number of times $\sin(\pi xs/p)$ is negative, i.e.,

$$(2k-1)\pi < \frac{\pi xs}{p} < 2k\pi \qquad \left(1 \leqq k < \frac{x+2}{4}\right),$$

where s ranges from 1 to $(p-1)/2$. In other words,
(2) *m_x is the number of integer s's which lie between $(2k-1)p/x$ and $2kp/x$ where $k=1, \cdots, [(x+1)/4]$, and is $< p/2$.*

From now on we assume $x \equiv 0 (\mathrm{mod}\, 2)$. Then $[(x+1)/4] \leqq x/4$. So in (2) we can omit the condition $s < p/2$.

From the above we have

$$\varepsilon^h = (-1)^{m_x} \prod_{s=1}^{(p-1)/2} (\zeta_x^s - \zeta_x^{-s})^{-\chi(xs)}$$
$$= (-1)^{m_x} \left(\prod_{k=1}^{g} \prod_{s \in I_k} (\zeta_x^s - \zeta_x^{-s})^{-\chi(s)} \right)^{\chi(x)}$$
$$= (-1)^{m_x} \left(\frac{\prod_{k=1}^{g} \prod_{n \in I_k} (\zeta_x^n - \zeta_x^{-n})}{\prod_{k=1}^{g} \prod_{r \in I_k} (\zeta_x^r - \zeta_x^{-r})} \right)^{\chi(x)} .$$

Since no pairs of $\pm gr (0 < r < p/2)$ are congruent mod p, n is congruent with some $\pm gr (0 < r < p/2)$. In fact, if $r \in I_{2a} (0 < a \leqq [g/2])$, then $(2a-1)p/2g < r < 2ap/2g$; so $0 < ap - gr < p/2$ and $n = ap - gr \equiv -gr (\mathrm{mod}\, p)$. Then

$$\zeta_x^n - \zeta_x^{-n} = -(\zeta_x^{gr} - \zeta_x^{-gr}) \qquad \text{for } x \equiv 0 \pmod 2 .$$

If $r \in I_{2a+1} (0 \leqq a \leqq [(g-1)/2])$, then $2ap/2g < r < (2a+1)p/2g$, so $0 < gr - ap < p/2$ and $n = gr - ap \equiv gr (\mathrm{mod}\, p)$. Then

$$\zeta_x^n - \zeta_x^{-n} = \zeta_x^{gr} - \zeta_x^{-gr} \qquad \text{for } x \equiv 0 \pmod 2 .$$

Consequently we get

$$\varepsilon^h=(-1)^{m_x}\left(\prod_{a=1}^{[g/2]}\frac{\prod_{n\equiv -gr, r\in I_{2a}}(\zeta_x^n-\zeta_x^{-n})}{\prod_{r\in I_{2a}}(\zeta_x^r-\zeta_x^{-r})}\prod_{a=0}^{[(g-1)/2]}\frac{\prod_{n\equiv gr, r\in I_{2a+1}}(\zeta_x^n-\zeta_x^{-n})}{\prod_{r\in I_{2a+1}}(\zeta_x^r-\zeta_x^{-r})}\right)^{\chi(x)}$$

$$=(-1)^{m_x}\left(\prod_{a=1}^{[g/2]}\prod_{r\in I_{2a}}\frac{-(\zeta_x^{gr}-\zeta_x^{-gr})}{(\zeta_x^r-\zeta_x^{-r})}\prod_{a=0}^{[(g-1)/2]}\prod_{r\in I_{2a+1}}\frac{(\zeta_x^{gr}-\zeta_x^{-gr})}{(\zeta_x^r-\zeta_x^{-r})}\right)^{\chi(x)}.$$

So we obtain the

PROPOSITION.

$$\varepsilon^h=(-1)^{m_x+u_g}\prod_{0<r<p/2}(\zeta_x^{(g-1)r}+\cdots+\zeta_x^{-(g-1)r})^{\chi(x)},$$

where u_g *is the number of r's contained in* $I_{2k}(k=1, \cdots, [g/2])$.

Next we shall prove the following

LEMMA 1.

$$u_g+v_g=\lambda_g,$$

where u_g *or* v_g *is the number of r's or n's contained in* I_{2k}*'s respectively when* $k=1, \cdots, [g/2]$.

PROOF. u_g+v_g is the number of integers contained in I_{2k}'s. And if $s\in I_{2k}$, then $(2k-1)p/2g<s<2kp/2g$. So $0<kp-sg<p/2$. Hence u_g+v_g is the number of multiples sg's whose smallest positive residues mod p are greater than $p/2$, when s ranges from 1 to $(p-1)/2$. Therefore $u_g+v_g=\lambda_g$.

COROLLARY 1.

$$\left(\frac{t+u\sqrt{p}}{2}\right)^h=(-1)^{v_g}\prod_{0<r<p/2}(\theta_g^{(g-1)r}+\cdots+\theta_g^{-(g-1)r})^{-\chi(2)} \tag{3}$$

$$\left(\frac{t-u\sqrt{p}}{2}\right)^h=(-1)^{v_g+1}\prod_{0<r<p/2}(\theta_g^{(g-1)r}+\cdots+\theta_g^{-(g-1)r})^{\chi(2)}. \tag{4}$$

PROOF. Setting $x=2g$ in our proposition, then from (2)

$$m_x=m_{2g}$$
$$=\left(\text{the number of } s\text{'s, where } \frac{(2k-1)p}{2g}<s<\frac{2kp}{2g},\right.$$
$$\left.\text{when } k=1, \cdots, \left[\frac{2g+1}{4}\right]\right)$$

$$=\left(\text{the number of } s\text{'s, where } s\in \mathrm{I}_{2k}, \text{ when } k=1, \cdots, \left[\frac{g}{2}\right]\right)$$

$$=u_g+v_g\ .$$

So

$$m_x+u_g=v_g+2u_g\equiv v_g \pmod 2\ .$$

Since $N\varepsilon=-1$ and h is odd, (3) implies (4).

COROLLARY 2.

$$(5)\qquad \left(\frac{t+u\sqrt{p}}{2}\right)^h=(-1)^{v_g+1}\prod_{0<r<p/2}(\theta^{(g-1)r}+\cdots+\theta^{-(g-1)r})^{\chi(2)}$$

$$(6)\qquad \left(\frac{t-u\sqrt{p}}{2}\right)^h=(-1)^{v_g}\prod_{0<r<p/2}(\theta^{(g-1)r}+\cdots+\theta^{-(g-1)r})^{-\chi(2)}\ .$$

PROOF. If we set $x=2$ in the proposition, then $m_x=m_2=0$. Since g is a quadratic non-residue mod p, λ_g is odd by Gauss's lemma (cf. [3] S. 95). So $m_x+u_g=u_g\equiv v_g+1 \pmod 2$ by Lemma 1.

If $p\equiv 5 \pmod 8$, i.e., $\chi(2)=-1$ (note $(p-1)/4\equiv 1 \pmod 2$), then from (3)

$$(7)\qquad \left(\frac{t+u\sqrt{p}}{2}\right)^h=-(-1)^{v_g+(p-1)/4}\prod_{0<r<p/2}(\theta_g^{(g-1)r}+\cdots+\theta_g^{-(g-1)r})$$

and from (6)

$$(8)\qquad \left(\frac{t-u\sqrt{p}}{2}\right)^h=-(-1)^{v_g+(p-1)/4}\prod_{0<r<p/2}(\theta^{(g-1)r}+\cdots+\theta^{-(g-1)r})\ .$$

If $p\equiv 1 \pmod 8$, i.e., $\chi(2)=1$ (note $(p-1)/4\equiv 0 \pmod 2$), then from (4)

$$(9)\qquad \left(\frac{t-u\sqrt{p}}{2}\right)^h=-(-1)^{v_g+(p-1)/4}\sum_{0<r<p/2}(\theta_g^{(g-1)r}+\cdots+\theta_g^{-(g-1)r})$$

and from (5)

$$(10)\qquad \left(\frac{t+u\sqrt{p}}{p}\right)^h=-(-1)^{v_g+(p-1)/4}\prod_{0<r<p/2}(\theta^{(g-1)r}+\cdots+\theta^{-(g-1)r})\ .$$

In each case, from (7) and (8), or (9) and (10)

$$(11)\qquad \left(\frac{t+u\sqrt{p}}{2}\right)^h+\left(\frac{t-u\sqrt{p}}{2}\right)^h$$

$$=-(-1)^{v_g+(p-1)/4}\left\{\prod_{0<r<p/2}(\theta^{(g-1)r}+\cdots+\theta^{-(g-1)r})\right.$$

$$\left.+\prod_{0<r<p/2}(\theta_g^{(g-1)r}+\cdots+\theta_g^{-(g-1)r})\right\}.$$

On the left side of (11), the part of $\sqrt{p}$ vanishes, therefore the left side is

$$2\left\{\left(\frac{t}{2}\right)^h+\frac{(\text{a multiple of } p)}{2^h}\right\}.$$

If we denote by $P(X)$ the polynomial

$$X^{p^2g^2}\left[2\left\{\left(\frac{t}{2}\right)^h+\frac{(\text{a multiple of } p)}{2^h}\right\}\right.$$

$$+(-1)^{v_g+(p-1)/4}\left\{\prod_{0<r<p/2}(X^{(g-1)r}+\cdots+X^{-(g-1)r})\right.$$

$$\left.\left.+\prod_{0<r<p/2}(X^{g(g-1)r}+\cdots+X^{-g(g-1)r})\right\}\right],$$

then $P(\theta)=0$, so $P(X)$ is divisible by

$$\frac{X^p-1}{X-1}=X^{p-1}+\cdots+X+1.$$

Setting $X=1$, since p is odd,

$$\left(\frac{t}{2}\right)^h\equiv-(-1)^{v_g+(p-1)/4}g^{(p-1)/4}\pmod{p}.$$

Since h is odd and $(t/2)^2\equiv-1(\text{mod}\, p)$, we get

$$(12)\qquad (-1)^{(h-1)/2}\frac{t}{2}\equiv-(-1)^{v_g+(p-1)/4}g^{(p-1)/4}\pmod{p}.$$

On the number v_g we now prove the following

LEMMA 2.

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

PROOF. Let λ'_g be the number of multiples sg's whose smallest positive residues mod p are smaller than $p/2$, when s ranges from 1 to $(p-1)/2$. And let u'_g or v'_g be the number of r's or n's contained in I_{2k-1}'s respectively. Then $u'_g+v'_g=\lambda'_g$ by a similar method of Lemma 1. Since

$$u'_g - v'_g = \sum_{k=1}^{[(g+1)/2]} \sum_{s \in I_{2k-1}} \left(\frac{s}{p}\right), \qquad v'_g = \frac{1}{2}\left\{\lambda'_g - \sum_{k=1}^{[(g+1)/2]} \sum_{s \in I_{2k-1}} \left(\frac{s}{p}\right)\right\}.$$

So

$$v_g = \frac{p-1}{4} - v'_g = \frac{p-1}{4} - \frac{1}{2}\left\{\lambda'_g - \sum_{k=1}^{[(g+1)/2]} \sum_{s \in I_{2k-1}} \left(\frac{s}{p}\right)\right\}$$
$$= \frac{1}{2}\left\{\left(\frac{p-1}{2} - \lambda'_g\right) + \sum_{k=1}^{[(g+1)/2]} \sum_{s \in I_{2k-1}} \left(\frac{s}{p}\right)\right\}.$$

Since $\lambda_g + \lambda'_g = (p-1)/2$,

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

From (12) and Lemma 2, we have Theorem 1.

§4. Proof of the Theorem 2.

$$P = \left(\frac{p-1}{2}\right)! = \prod_{0<r<p/2} r \prod_{0<n<p/2} n$$
$$= \prod_{0<r<p/2} r \prod_{1 \le k \le g} \prod_{n \in I_k} n$$
$$= \prod_{0<r<p/2} r \left(\prod_{k=1}^{[(g+1)/2]} \prod_{n \in I_{2k-1}} n\right)\left(\prod_{k=1}^{[g/2]} \prod_{n \in I_{2k}} n\right).$$

The method of the proof in the proposition in §3 follows

$$P \equiv \prod_{0<r<p/2} r \left(\prod_{k=1}^{[(g+1)/2]} \prod_{\substack{r \equiv ng \\ n \in I_{2k-1} \\ 0<r<p/2}} \frac{r}{g}\right)\left(\prod_{k=1}^{[g/2]} \prod_{\substack{-r \equiv ng \\ n \in I_{2k} \\ 0<r<p/2}} \frac{-r}{g}\right)$$
$$\equiv \frac{(-1)^{v_g}}{g^{(p-1)/4}}\left(\prod_{0<r<p/2} r\right)^2 \pmod{p},$$

where v_g is the number of n's contained in I_{2k}'s. Since $(\prod_{0<r<p/2} r)^2 \equiv -(-1)^{(p-1)/4} \pmod{p}$ (cf. [1]) and $g^{(p-1)/2} \equiv -1 \pmod{p}$, we get

$$P \equiv \frac{-(-1)^{(p-1)/4+v_g}}{g^{(p-1)/4}} \equiv (-1)^{(p-1)/4+v_g} g^{(p-1)/4} \pmod{p}.$$

Hence

$$\frac{((p-1)/2)!}{g^{(p-1)/4}} \equiv (-1)^{(p-1)/4+v_g} \pmod{p},$$

which is Theorem 2.

§5. **The number λ_g and v_g.**

In connection with two different quadratic non-residues modulo p, we get the following supplemental result which will be used for calculation. Let g_1, g_2 be two positive quadratic non-residues modulo p such that $g_1+g_2=p$ (therefore g_1 and g_2 are different and $0<g_1, g_2<p$). From Theorem 1, we can easily get

$$v_{g_1}+v_{g_2}\equiv\frac{p-1}{4} \pmod 2 .$$

But we can prove directly (without using Theorem 1) the following more precise

LEMMA 3. *Let g_1, g_2 be two positive quadratic non-residues modulo p such that $g_1+g_2=p$. Then*

$$1)\quad \lambda_{g_1}+\lambda_{g_2}=\frac{p-1}{2}$$

$$2)\quad v_{g_1}+v_{g_2}=\frac{p-1}{4} .$$

PROOF. 1) Write $I_{2k}^{(1)}=((2k-1)p/2g_1, 2kp/2g_1)$, then

$$\begin{aligned} s\in I_{2k}^{(1)} &\Leftrightarrow \frac{(2k-1)p}{2g_1}<s<\frac{2kp}{2g_1} \\ &\Leftrightarrow 0<kp-sg_1<\frac{p}{2} \\ &\Leftrightarrow 0<kp-s(p-g_2)<\frac{p}{2} \\ &\Leftrightarrow (s-k)p<sg_2<(s-k)p+\frac{p}{2} \\ &\Leftrightarrow \frac{(2k'-2)p}{2g_2}<s<\frac{(2k'-1)p}{2g_2} \quad (k'+k=s+1) \\ &\Leftrightarrow s\in I_{2k'-1}^{(2)}=\left(\frac{(2k'-2)p}{2g_2}, \frac{(2k'-1)p}{2g_2}\right) . \end{aligned}$$

Hence $\lambda_{g_1}=\lambda'_{g_2}$. Similarly $\lambda_{g_2}=\lambda'_{g_1}$. Since $\lambda_{g_1}+\lambda'_{g_1}=(p-1)/2$, so we get $\lambda_{g_1}+\lambda_{g_2}=(p-1)/2$.

2) From what has been proved above,

$$\sum_{k=1}^{[(g_1+1)/2]}\sum_{s\in I_{2k-1}^{(1)}}\left(\frac{s}{p}\right)+\sum_{k=1}^{[(g_2+1)/2]}\sum_{s\in I_{2k-1}^{(2)}}\left(\frac{s}{p}\right)$$

$$=\sum_{k=1}^{[(g_1+1)/2]}\sum_{s\in I_{2k-1}^{(1)}}\left(\frac{s}{p}\right)+\sum_{k=1}^{[g_1/2]}\sum_{s\in I_{2k}^{(1)}}\left(\frac{s}{p}\right)=\sum_{0<s<p/2}\left(\frac{s}{p}\right)=0 .$$

So we get

$$\begin{aligned} v_{g_1}+v_{g_2} &= \frac{1}{2}\left\{\lambda_{g_1}+\sum_{k=1}^{[(g_1+1)/2]}\sum_{s\in I_{2k-1}}\left(\frac{s}{p}\right)\right\}+\frac{1}{2}\left\{\lambda_{g_2}+\sum_{k=1}^{[(g_2+1)/2]}\sum_{s\in I_{2k-1}}\left(\frac{s}{p}\right)\right\} \\ &= \frac{1}{2}(\lambda_{g_1}+\lambda_{g_2})=\frac{p-1}{4} . \end{aligned}$$

References

[1] P. Chowla, On the class-number of real quadratic fields, Journal für Mathematik, Bd **230** (1968), 51-60.

[2] P. Chowla and S. Chowla, Formulae for units and class-numbers of real quadratic fields, Journal für Mathematik, Bd **230** (1968), 61-65.

[3] H. Hasse, Vorlesungen über Zahlentheorie, Berlin, 1950.

Present Address:
College of Industrial Technology
Nihon University
Izumi-cho, Narashino-shi
Chiba 275