# ON THE DISTRIBUTION OF IDEAL CLASS NUMBERS \(h\) OF REAL QUADRATIC FIELDS \(K(\sqrt p)\) WITH PRIME DISCRIMINANT \(p \equiv 1 \pmod 4\) AMONG THE RESIDUE CLASSES \(\{4k+1\}\) AND \(\{4k+3\}\)

MATHEMATICS

1968

## Abstract

## Full Text

UDC 511.6

*MATHEMATICS*

**V. G. LEMMERMEYEN**

# ON THE DISTRIBUTION OF IDEAL CLASS NUMBERS $h$ OF REAL QUADRATIC FIELDS $K(\sqrt{p})$ WITH PRIME DISCRIMINANT $p \equiv 1 \pmod 4$ AMONG THE RESIDUE CLASSES $\{4k+1\}$ AND $\{4k+3\}$

*(Presented by Academician P. S. Novikov on June 2, 1967)*

Let the prime $p \equiv 1 \pmod 4$. Then the natural numbers $a$ and $b$ are uniquely determined by the condition $a^2 + b^2 = p$, where $a \equiv 1 \pmod 2$, $b \equiv 0 \pmod 2$. It is known that the ideal class number $h$ of the field $K(\sqrt{p})$ is odd, and one of the congruences

$$a\mathfrak{A} \pm b\mathfrak{B} \equiv 0 \pmod p,$$

is always satisfied, where

$$\mathfrak{A} = \prod_{\nu=1}^{(p-1)/4} a_\nu \quad \text{and} \quad \mathfrak{B} = \prod_{\nu=1}^{(p-1)/4} b_\nu,$$

the products of the quadratic residues $a_\nu$ and nonresidues $b_\nu$ from the least positive half-system

$$1, 2, \ldots, (p-1)/2.$$

**Theorem 1.** The positive number

$$\tau = \sqrt{\frac{(-1)^{(a-1)/2}a + \sqrt{p}}{2\varepsilon}}$$

$$\left(\sigma = \sqrt{\frac{(-1)^{(a-1)/2}a - \sqrt{p}}{2\varepsilon'}}\right),$$

where $\varepsilon$ is the fundamental unit of $K(\sqrt{p})$ ($\varepsilon$ and $\varepsilon'$ are mutually conjugate), is an integer in $K(\sqrt{p})$, and $\operatorname{sgn} N(\tau)$ ($\operatorname{sgn} N(\sigma)$) can be equal both to $+1$ and to $-1$.

**Proof.** Let $\eta = \varepsilon^h$ be the circular unit of $K(\sqrt{p})$. According to Hasse's theorem ([1]) on the rational representation $\eta = (u + v\sqrt{p})/2$,

$$u = A(A_1^2 - B_1^2) - 2BA_1B_1, \tag{1}$$

$$v = A_1^2 + B_1^2. \tag{2}$$

Here $A_1$ and $B_1$ are expressed as sums

$$A_1 = \sum e_1 \cdots e_n, \qquad B_1 = \sum e_1 \cdots e_n \quad \left(n = \frac{p-1}{4}\right),$$

extended over all possible solutions of the congruences

$$\sum_{i=1}^{n} a_i e_i \equiv 1 \pmod{p}$$

and, respectively,

$$\sum_{i=1}^{n} b_i e_i \equiv 1 \pmod{p}$$

in the units $e_i = \pm 1$, while $A$ and $B$ are uniquely determined by the conditions

$$A \equiv 1 \pmod{4}, \qquad B \equiv 0 \pmod{2},$$

$$A\mathfrak{A} + B\mathfrak{B} \equiv 0 \pmod{p} \quad (A^2 + B^2 = p).$$

Hasse' s idea of proof consists in the evaluation of the normalized Gauss sums $\tau(\chi)$ and $\tau(\bar{\chi})$, belonging to the complex conjugate biquadratic characters $\chi$ and $\bar{\chi}$. Such sums arise when considering the products

$$\prod_{\nu=1}^{n} (\zeta_2^{a_\nu} - \zeta_2^{-a_\nu}) = \frac{\chi(2)\tau(\chi)(A_1 + B_1 i) + \bar{\chi}(2)\tau(\bar{\chi})(A_1 - B_1 i)}{2}, \tag{3}$$

$$\prod_{\nu=1}^{n} \left(\zeta_2^{b_\nu} - \zeta_2^{-b_\nu}\right) = \frac{\chi(2)\tau(\chi)(A_1 + B_1 i) - \bar{\chi}(2)\tau(\bar{\chi})(A_1 - B_1 i)}{2i}. \tag{4}$$

which make it possible to express the circular unit of $K(\sqrt{p})$ in the form

$$\eta = (-1)^n \prod_{\nu=1}^{n} \left(\zeta_2^{-b_\nu} - \zeta_2^{b_\nu}\right) \Big/ \prod_{\nu=1}^{n} (\zeta_2^{a_\nu} - \zeta_2^{-a_\nu}).$$

Here $\zeta_2 = \zeta^{(p+1)/2}$, $\left(\zeta = e^{2\pi i/p}\right)$.

Let us also note that

$$\chi^2(2) = \overline{\chi}^2(2) = \left(\frac{2}{p}\right) = (-1)^n, \tag{5}$$

$$\tau^2(\chi) = -(A + Bi)\sqrt{p}, \tag{6}$$

$$\tau^2(\overline{\chi}) = -(A - Bi)\sqrt{p}. \tag{7}$$

The derivation of relations (3), (4), as well as (5), (6), and (7), may be found in the monograph ([1]).

We shall first show that the numbers $A, B, A_1$, and $B_1$ are connected by the relation

$$B(A_1^2 - B_1^2) + A(2A_1B_1) = (-1)^{n+1} \cdot 2. \tag{8}$$

Indeed, multiplying (3) and (4) term by term, on the left we shall have

$$\prod_{\nu=1}^{n} (\zeta_2^{a_\nu} - \zeta_2^{-a_\nu}) \prod_{\nu=1}^{n} \left(\zeta_2^{b_\nu} - \zeta_2^{-b_\nu}\right) = \prod_{x=1}^{2n} (\zeta_2^x - \zeta_2^{-x}) = \sqrt{p},$$

and on the right

$$\left[\chi^2(2)\tau^2(\chi)(A_1 + B_1 i)^2 - \overline{\chi}^2(2)\tau^2(\overline{\chi})(A_1 - B_1 i)^2\right]/4i.$$

Taking now (5), (6), and (7) into account, we obtain

$$(-1)^{n+1}(A + Bi)(A_1 + B_1 i)^2 - (-1)^{n+1}(A - Bi)(A_1 - B_1 i)^2 = 4i,$$

which is, evidently, equivalent to (8). Let us note in passing that the relation $N(\eta) = -1$, which, as is known, always holds in the $K(\sqrt{p})$ under consideration, does not entail any new dependence among $A, B, A_1$, and $B_1$. The corresponding relation $[B(A_1^2 - B_1^2) + A(2A_1B_1)]^2 = 4$ is simply a consequence of (8).

From (1), (2), and (8) we obtain

$$A_1^2 = v/2 + [Au + (-1)^{n+1}2B]/2p,$$

$$B_1^2 = v/2 - [Au + (-1)^{n+1}2B]/2p$$

or

$$\begin{aligned} A_1^2 &= \frac{\sqrt{p}}{2p}(\varepsilon^h - \varepsilon'^h) + (-1)^{n+1}\frac{B}{p} + \frac{A}{2p}(\varepsilon^h + \varepsilon'^h), \\ B_1^2 &= \frac{\sqrt{p}}{2p}(\varepsilon^h - \varepsilon'^h) - (-1)^{n+1}\frac{B}{p} - \frac{A}{2p}(\varepsilon^h + \varepsilon'^h). \end{aligned} \tag{9}$$

Further, since $A = (-1)^{(a-1)/2}a$, and $B = \operatorname{sgn} B \cdot b$, the relations (9) may be rewritten in the form

$$A_1^2 = \frac{1}{p}\left(\frac{(-1)^{(a-1)/2}a + \sqrt{p}}{2\varepsilon}\,\varepsilon^{h+1} + (-1)^{n+1}\operatorname{sgn} B \cdot b + \frac{(-1)^{(a-1)/2}a - \sqrt{p}}{2\varepsilon'}\,\varepsilon^{-(h+1)}\right),$$

$$B_1^2 = \frac{1}{p}\left(\frac{(-1)^{(a-1)/2}a - \sqrt{p}}{2\varepsilon'}\,\varepsilon^{h-1} - (-1)^{n+1}\operatorname{sgn} B \cdot b + \frac{(-1)^{(a-1)/2}a + \sqrt{p}}{2\varepsilon}\,\varepsilon^{-(h-1)}\right).$$

Introducing, finally, the positive

$$\sigma = \sqrt{\frac{(-1)^{(a-1)/2}a - \sqrt{p}}{2\varepsilon'}} \quad \text{and} \quad \tau = -\sqrt{\frac{(-1)^{(a-1)/2}a + \sqrt{p}}{2\varepsilon}},$$

we obtain

$$\begin{aligned} |A_1|\sqrt{p} &= \left|\tau\varepsilon^{(h+1)/2} - (-1)^n \operatorname{sgn} B \cdot \sigma\varepsilon^{-(h+1)/2}\right|, \\ |B_1|\sqrt{p} &= \left|\sigma\varepsilon^{(h-1)/2} + (-1)^n \operatorname{sgn} B \cdot \tau\varepsilon^{-(h-1)/2}\right|. \end{aligned} \tag{10}$$

For $(-1)^n \operatorname{sgn} B = -1$ ($(-1)^n \operatorname{sgn} B = +1$), the numbers $\tau\varepsilon^{(h+1)/2}$ and $\sigma\varepsilon^{-(h+1)/2}$ ($\sigma\varepsilon^{(h-1)/2}$ and $\tau\varepsilon^{-(h-1)/2}$) are roots of the equation

$$x^2 - |A_1|\sqrt{p}\,x + b/2 = 0, \qquad \left(x^2 - |B_1|\sqrt{p}\,x + b/2 = 0\right), \tag{11}$$

whose discriminant $A_1^2 p - 2b$ ($B_1^2 p - 2b$) must be the square of some natural number $M$ ($N$), since $\tau^2\varepsilon^{h+1}$ and $\sigma^2\varepsilon^{-(h+1)}$ ($\sigma^2\varepsilon^{h-1}$ and $\tau^2\varepsilon^{-(h-1)}$) are integers in $K(\sqrt{p})$, while $A_1^2 p - 2b$ ($B_1^2 p - 2b$) is not divisible by $p$.

The fact that the number $\tau$, as well as $\sigma$, is an integer in $K(\sqrt{p})$ now follows directly from (11) and from the obvious fact that $A_1$ and $M$ ($B_1$ and $N$) are numbers of the same parity.

Next, in $K(\sqrt{p})$ with prime $p = a^2 + 4$ ($a > 0$), the fundamental unit is

$$\varepsilon = (a + \sqrt{p})/2.$$

Thus, for $a \equiv 1 \pmod 4$, the number $\tau = 1$ ($\sigma = 1$) and, consequently, $\operatorname{sgn} N(\tau) = +1$ ($\operatorname{sgn} N(\sigma) = +1$), while for $a \equiv 3 \pmod 4$,

$$\tau = (-a + \sqrt{p})/2 \quad (\sigma = (a + \sqrt{p})/2)$$

and $\operatorname{sgn} N(\tau) = -1$ ($\operatorname{sgn} N(\sigma) = -1$).

**Theorem 2.** *The residue class modulo 4 to which the ideal class number $h$ of $K(\sqrt{p})$, with prime $p \equiv 1 \pmod 4$, belongs is uniquely determined by conditions I and II according to the table:*

| II I | $\mathfrak{A}a+\mathfrak{B}b\equiv 0 \pmod p$ | $\mathfrak{A}a-\mathfrak{B}b\equiv 0 \pmod p$ |
|---|---|---|
| $\operatorname{sgn} N(\tau)=(-1)^{(a+b+1)/2}$ | $h\equiv 1 \pmod 4$ | $h\equiv 3 \pmod 4$ |
| $\operatorname{sgn} N(\tau)=-(-1)^{(a+b+1)/2}$ | $h\equiv 3 \pmod 4$ | $h\equiv 1 \pmod 4$ |

**Proof.** Since the numbers $\tau$ and $\sigma$ are connected by the relation

$$\tau=\operatorname{sgn} N(\sigma)\sigma', \qquad \sigma=\operatorname{sgn} N(\tau)\tau',$$

and, obviously,

$$\varepsilon^{-(h+1)/2}=(-1)^{(h+1)/2}(\varepsilon')^{(h+1)/2}, \qquad \varepsilon^{-(h-1)/2}=(-1)^{(h-1)/2}(\varepsilon')^{(h-1)/2},$$

the equalities (10) transform into

$$|A_1|\sqrt{p}=\left|\tau\varepsilon^{(h+1)/2}-(-1)^{n+(h+1)/2}\operatorname{sgn}(BN(\tau))\tau'(\varepsilon')^{(h+1)/2}\right|,$$
$$|B_1|\sqrt{p}=\left|\sigma\varepsilon^{(h-1)/2}-(-1)^{n+(h+1)/2}\operatorname{sgn}(BN(\sigma))\sigma'(\varepsilon')^{(h-1)/2}\right|.$$

Hence, taking into account that $\operatorname{sgn} N(\tau)=\operatorname{sgn} N(\sigma)$, we obtain

$$(-1)^n\operatorname{sgn}(B\cdot N(\tau))=(-1)^{(h+1)/2}. \tag{12}$$

Furthermore, the congruence $A\mathfrak{A}+B\mathfrak{B}\equiv 0 \pmod p$, when rewritten in the form

$$(-1)^{(a-1)/2}a\mathfrak{A}+\operatorname{sgn} B\cdot b\mathfrak{B}\equiv 0 \pmod p,$$

shows that the conditions

$$\mathfrak{A}a+\mathfrak{B}b\equiv 0 \pmod p, \qquad \mathfrak{A}a-\mathfrak{B}b\equiv 0 \pmod p \tag{13}$$

are respectively equivalent to

$$\operatorname{sgn} B=(-1)^{(a-1)/2}, \qquad \operatorname{sgn} B=-(-1)^{(a-1)/2}.$$

Thus, when the first of relations (13) holds, equality (12) takes the form:

$$(-1)^{(p+2a-3)/4}\operatorname{sgn} N(\tau)=(-1)^{(h+1)/2}.$$

and, consequently, the conditions

$$\operatorname{sgn} N(\tau)=\pm(-1)^{(a+b+1)/2} \tag{14}$$

lead respectively to

$$(-1)^{[(a+2)^2+(b+1)^2-6]/4} = \pm(-1)^{(h+1)/2},$$

which, in view of the obvious congruence $(a+2)^2+(b+1)^2 \equiv 2 \pmod 8$, gives $h \equiv 1 \pmod 4$ and $h \equiv 3 \pmod 4$.

The case in which the second of conditions (13) is satisfied is considered analogously.

Let us also note that each of the relations (14) can in fact occur. For example, for a prime $p = 1+b^2 > 5$, the fundamental unit of $K(\sqrt{p})$ is $\varepsilon = b+\sqrt{1+b^2}$, the number $\tau = (b-1+\sqrt{1+b^2})/2$, and therefore $\operatorname{sgn} N(\tau) = -1$. Hence it is clear that for $b \equiv 0 \pmod 4$ the first of conditions (14) is satisfied, while for $b \equiv 2 \pmod 4$ the second is satisfied.

As a consequence of Theorem 2 we obtain the congruence

$$a\mathfrak{A} + (-1)^{(a+b+h)/2} \operatorname{sgn} N(\tau)\, b\mathfrak{B} \equiv 0 \pmod p.$$

The question of the extent to which the theorems obtained can be extended to real quadratic fields $K(\sqrt{d})$ with composite discriminant remains open for the time being. However, Hasse' s method ([1]), which is used essentially here, was generalized to fields $K(\sqrt{d})$ with composite $d$ by Bergström ([2]).

Moscow State
Pedagogical Institute
named after V. I. Lenin

Received
2 VI 1967

## REFERENCES

[1] H. Hasse, *Lectures on Number Theory*, IL, 1953, pp. 443-455. [2] H. Bergström, *J. Math.*, **186**, 91 (1945).

*Note: Figure translations are in progress. See original paper for figures.*