ON THE 2-CLASS NUMBER OF CERTAIN QUADRATIC NUMBER FIELDS

By

Akira ENDÔ

(Received Oct. 20, 1972)

Recently Reichardt [5] studied the 2-class number of quadratic number fields whose discriminants are products of two prime discriminants. Basing upon his earlier work [4], Reichardt obtained there a criterion of the divisibility by 2^3 of the class number of such quadratic number fields. It is a criterion in the ring of rational integers, but is slightly different from the Hasse's ones which are given by using the genus theory in [1] and [2].

In this note we shall extend the Reichardt's results to the case of quadratic fields whose discriminants are even and contain two prime factors besides 2.

Both an ideal class group and a class number always mean ones in the narrow sense.

1. Known results

First, we shall provide some results from [3] and [4] without proof.

Let $K=Q(\sqrt{d})$ be a quadratic number field with discriminant d , where Q means the field of rational numbers.

In this note a decomposition of the discriminant d always means a decomposition of d into a product of two discriminants d_1 and d_2 of quadratic number fields. Two decompositions $d=d_1d_2$ and $d=d_2d_1$ are considered the same one. With regard to a decomposition of d , we have the following

DEFINITION ([4]). A decomposition $d=d_1d_2$ of d is called to be of the n -th kind, if there exists an unramified cyclic extension of K of degree 2^n including $Q(\sqrt{d_1}, \sqrt{d_2})$ as an intermediate field, or equivalently,

if there exists an unramified cyclic extension of K of degree 2^{n-1} , in which all the prime ideals of K dividing d split completely, including $Q(\sqrt{d_1}, \sqrt{d_2})$ as an intermediate field.

If we define the product of two decompositions $d = d_1 d_2$ and $d = d'_1 d'_2$ by $d = d''_1 d''_2$ where d''_1 and d''_2 are respectively the square free kernels of $d_1 d'_1$ and $d_2 d'_2$, then all of the decompositions of d forms a commutative group of type $(2, \dots, 2)$ having the trivial decomposition $d = 1 \cdot d$ as the identity. And furthermore, all of the decompositions of the n -th kind forms its subgroup ([4]).

Now, let r_n denote the number of factors which occur in a direct decomposition of the ideal class group of K into cyclic primary components, and whose orders are divisible by 2^n . Then we have the following

PROPOSITION 1 ([4]). r_n is equal to the maximal number of independent decompositions of d which are of the n -th kind.

A decomposition of d which is of the second kind or of the third kind is characterized as follows.

PROPOSITION 2 ([3], [4]). (1) A decomposition $d = d_1 d_2$ is of the second kind if and only if for every prime number dividing $d d_i^{-1}$

$$\left(\frac{d_i}{p}\right) = 1, \quad i = 1, 2,$$

where $\left(\frac{d_i}{p}\right)$ is the Jacobi-Kronecker symbol.

(2) Suppose that $d = d_1 d_2$ is a decomposition of the second kind. Then the diophantine equation $x^2 - d_1 y^2 - d_2 z^2 = 0$ has a non-trivial solution such that $\alpha = x + y\sqrt{d_1}$ is not primary for the one and only prime ideal in each class of two conjugate prime ideals of $Q(\sqrt{d_1})$ dividing d_2 , and is primary for all other prime ideals of $Q(\sqrt{d_1})$. And besides, K_2 is an unramified cyclic extension of K of degree 2^2 including $K_1 = Q(\sqrt{d_1}, \sqrt{d_2})$ as an intermediate field, if and only if K_2 takes the form of $K_1(\sqrt{\alpha d'})$ where d' runs over all the factors which occur in decompositions of d .

(3) Under the situation above, $d = d_1 d_2$ is furthermore a decomposition of the third kind, if and only if there exists at least one factor d' which occurs in a decomposition of d , such that if $\mathfrak{p}$ is a prime ideal of

$Q(\sqrt{d_1})$ dividing d for which $\alpha d'$ is primary, then $\alpha d'$ is furthermore hyperprimary for $\mathfrak{p}$.

In the last statement, in case where $\alpha d'$ is prime to $\mathfrak{p}$, $\alpha d'$ is hyperprimary for $\mathfrak{p}$, if and only if $\alpha d'$ is a quadratic residue modulo $\mathfrak{p}^5$ or modulo $\mathfrak{p}$ according as $\mathfrak{p}$ divides 2 or not.

2. Some lemmas

In what follows, suppose that d has a decomposition $d = d_1 d_2$ of the second kind, and besides that d_1 is even. Then the diophantine equation

$$x^2 - d_1 y^2 - d_2 z^2 = 0$$

has a non-trivial solution satisfying

$$(x, y, z) = 1 \text{ and } x + 2y \equiv 1 \pmod{4}.$$

And put

$$\alpha = x + y\sqrt{d_1}.$$

Then we see that $K_2 = K_1(\sqrt{\alpha})$, where $K_1 = Q(\sqrt{d_1}, \sqrt{d_2})$, is a cyclic extension of K , and we have that α satisfies the condition in (2) of Theorem 2, if and only if α is a quadratic residue modulo 4 in K_1 ([3]). In fact, this is the case, as shown in the following

LEMMA 1.

$$\alpha \equiv (1 + y\sqrt{d_1/4})^2 \pmod{4}.$$

PROOF. It follows immediately from the assumption and (1) of Proposition 2 that $d_1 \equiv 0 \pmod{4}$, $d_2 \equiv 1 \pmod{8}$, and $x \equiv z \equiv 1 \pmod{2}$. Put now $d_1 = 4m$, where $m \equiv 2, -1 \pmod{4}$. Since $4my^2 = x^2 - d_2 z^2 \equiv 0 \pmod{8}$, we have $my \equiv 0 \pmod{2}$ and hence $2y + my^2 \equiv 0 \pmod{4}$. It follows that $x - (1 + my^2) \equiv x + 2y - 1 \equiv 0 \pmod{4}$ and hence $\alpha \equiv (1 + y\sqrt{m})^2 \pmod{4}$.

Now, let $\mathfrak{z}$ denote the unique prime ideal of $Q(\sqrt{d_1})$ which divides 2.

LEMMA 2. (1) For any $\beta \in Q(\sqrt{d_1})$ satisfying $\beta \equiv \alpha \pmod{4}$, β is a quadratic residue modulo $\mathfrak{z}^5$, if and only if $\beta \equiv (1 + y\sqrt{d_1/4})^2 \pmod{\mathfrak{z}^5}$.

(2) For any rational integer d' satisfying $d' \equiv 1 \pmod{4}$, $d'\alpha$ is a quadratic residue modulo $\mathfrak{z}^5$, if and only if $x \equiv d' + (d_1/4)y^2 \pmod{8}$.

PROOF. (1) Put now $\beta \equiv (a + b\sqrt{m})^2 \pmod{\mathfrak{z}^5}$, $m = d_1/4$. It follows from $\beta \equiv \alpha \equiv (1 + y\sqrt{m})^2 \pmod{4}$ that $a^2 - 1 + (b^2 - y^2)m \equiv 0 \pmod{4}$ and $y \equiv ab \pmod{2}$, and hence $(a^2 - 1)(1 - b^2m) \equiv 0 \pmod{4}$. Since $m \equiv 2, -1 \pmod{4}$, we have $b^2m \not\equiv 1 \pmod{4}$ and $a \equiv 1 \pmod{2}$. Here we may assume $a \equiv 1 \pmod{4}$, and we can put $b = y + 2b'$. Then, $(a + b\sqrt{m})^2 - (1 + y\sqrt{m})^2 \equiv 4b'((b' + y)m + \sqrt{m}) \pmod{8}$, and besides $(b'((b' + y)m + \sqrt{m}))(b'((b' + y)m - \sqrt{m})) = b'^2((b' + y)^2m^2 - m) \equiv b'(b' - 1)m \equiv 0 \pmod{2}$ because $my \equiv 0 \pmod{2}$. Hence $b'((b' + y)m + \sqrt{m}) \equiv 0 \pmod{\mathfrak{z}}$ and $(a + b\sqrt{m})^2 \equiv (1 + y\sqrt{m})^2 \pmod{\mathfrak{z}^5}$.

(2) Clearly we have $d'\alpha \equiv \alpha \pmod{4}$. It follows from (1) that $d'\alpha$ is a quadratic residue modulo $\mathfrak{z}^5$, if and only if $d'\alpha \equiv (1 + y\sqrt{m})^2 \pmod{\mathfrak{z}^5}$. Here $d'\alpha - (1 + y\sqrt{m})^2 = d'(x + 2y\sqrt{m}) - (1 + y\sqrt{m})^2 \equiv d'x - 1 - my^2 \pmod{8}$ because $d' \equiv 1 \pmod{4}$. Hence $d'\alpha$ is a quadratic residue modulo $\mathfrak{z}^5$, if and only if $d'x \equiv 1 + my^2 \pmod{8}$. Since $my \equiv 0 \pmod{2}$, $d'x \equiv 1 + my^2 \pmod{8}$ if $x \equiv d' + my^2 \pmod{8}$, and conversely. Hence the lemma follows.

LEMMA 3 ([5]). Let $p \neq 2$ be a prime number which is a divisor of d and $\mathfrak{p}$ a prime ideal of $Q(\sqrt{d_1})$ which divides p . And let d' be a rational integer prime to p .

(1) Suppose now that p ramifies in $Q(\sqrt{d_1})$, namely, p is a divisor of d_1 . Then $d'\alpha$ is a quadratic residue modulo $\mathfrak{p}$, if and only if $\left(\frac{d'x}{p}\right) = 1$.

(2) Suppose next that p splits in $Q(\sqrt{d_1})$, namely, p is a divisor of d_2 , and besides that α is prime to $\mathfrak{p}$. Then $d'\alpha$ is a quadratic residue modulo $\mathfrak{p}$, if and only if $\left(\frac{d'x}{p}\right) = \left(\frac{2}{p}\right)$.

PROOF. (1) Since $\alpha = x + y\sqrt{d_1} \equiv x \pmod{\mathfrak{p}}$, $d'\alpha$ is a quadratic residue modulo $\mathfrak{p}$, if and only if $d'x$ is a quadratic residue modulo $\mathfrak{p}$. And since the degree of $\mathfrak{p}$ is one, $d'x$ is a quadratic residue modulo $\mathfrak{p}$, if and only if $d'x$ is a quadratic residue modulo p , that is, $\left(\frac{d'x}{p}\right) = 1$.

(2) Let α' denote the conjugate of α and $\mathfrak{p}'$ the conjugate of $\mathfrak{p}$. It is clear that $\alpha \equiv 0 \pmod{\mathfrak{p}'}$ and $\alpha' \equiv 0 \pmod{\mathfrak{p}}$. Then $d'\alpha$ is a quadratic residue modulo $\mathfrak{p}$, if and only if $2d'x = d'\alpha + d'\alpha'$ is a quadratic residue modulo $\mathfrak{p}$. And since the degree of $\mathfrak{p}$ is also one, $2d'x$ is a quadratic

residue modulo p , if and only if $2d'x$ is a quadratic residue modulo p , that is, $\left(\frac{d'x}{p}\right) = \left(\frac{2}{p}\right)$.

From now on suppose that d contains exactly two other prime factors, denoted by p and q , than 2.

Here we note that d_1 and d_2 are not both negative from the law of reciprocity.

We have, in general, $\left(\frac{d_2}{|x|}\right) = \left(\frac{d_2 z^2}{|x|}\right) = \left(\frac{x^2 - d_1 y^2}{|x|}\right) = \left(\frac{-d_1 y^2}{|x|}\right) = \left(\frac{-d_1}{|x|}\right)$ and hence $1 = \left(\frac{-d_1}{|x|}\right) \left(\frac{d_2}{|x|}\right) = \left(\frac{-d}{|x|}\right) = \left(\frac{\pm pq}{|x|}\right)$ or $\left(\frac{\pm 2pq}{|x|}\right)$. From this we have easily the following

LEMMA 4. (1) In the case $d_1 = -4$, $\left(\frac{x}{p}\right) = \left(\frac{x}{q}\right)$ is always satisfied.

(2) In the case $d_1 = -8$, $\left(\frac{x}{p}\right) = \left(\frac{x}{q}\right)$ if and only if $x \equiv \pm 1 \pmod{8}$.

(3) In the case $d_1 = 8$, $\left(\frac{x}{p}\right) = \left(\frac{x}{q}\right)$ if and only if $|x| \equiv 1, 3 \pmod{8}$ or $x \equiv 1, 3 \pmod{8}$ according to $d > 0$ or not.

(4) In the case $d < 0$ and $|d_1| = 4p$, $\left(\frac{x}{p}\right) = \left(\frac{x}{q}\right)$ is always satisfied.

And in the case $d > 0$ and $d_1 = 4p$, $\left(\frac{x}{p}\right) = \left(\frac{x}{q}\right)$ if and only if $x > 0$.

(5) In the case $d < 0$ and $|d_1| = 8p$, $\left(\frac{x}{p}\right) = \left(\frac{x}{q}\right)$ if and only if $x \equiv 1, 3 \pmod{8}$ or $x \equiv \pm 1 \pmod{8}$ according to $d_1/8 \equiv 1 \pmod{4}$ or not. And in the case $d > 0$ and $d_1 = 8p$, $\left(\frac{x}{p}\right) = \left(\frac{x}{q}\right)$ if and only if $|x| \equiv 1, 3 \pmod{8}$ or $x \equiv \pm 1 + 2(1 - \text{sgn}(x)) \pmod{8}$ according to $p \equiv 1 \pmod{4}$ or not.

In the following we shall study conditions for that the discriminant d has a decomposition of the third kind.

Here we note that if d' is a factor which occurs in a decomposition of d , then $K_1(\sqrt{d'\alpha}) = K_1(\sqrt{d''\alpha})$ where d'' is the square free kernel of $d'd_1$ or $d'd_2$.

3. The case where d is not a multiple of 8

Now, suppose that d is divisible by exactly 2^2 : $d = \pm 4pq$. It follows

from (1) of Proposition 2 that $r_2 \geq 1$, namely, d has a decomposition of the second kind, if and only if at least one of the following conditions is satisfied:

$$p \equiv q \equiv 1, 5 \pmod{8} \quad (d_1 = -4, d_2 = pq)$$

$$p \equiv 1 \pmod{4}, q \equiv 1 \pmod{8} \text{ and } \left(\frac{p}{q}\right) = 1 \quad (d_1 = -4p, d_2 = q)$$

$$p \equiv -1 \pmod{4}, q \equiv \pm 1 \pmod{8} \text{ and } \left(\frac{p}{q}\right) = 1 \quad (d_1 = 4p, d_2 = \pm q)$$

In particular, $r_2 = 2$, namely, decompositions of d are all of the second kind, if and only if $p \equiv q \equiv 1 \pmod{8}$ and $\left(\frac{p}{q}\right) = 1$.

THEOREM 1. (1) *Let $p \equiv q \equiv 1, 5 \pmod{8}$. Then $d_1 = -4$ and $d_2 = pq$ define a decomposition of d which is of the third kind, if and only if one of the following conditions is satisfied:*

$$p \equiv q \equiv 1 \pmod{8}, x + 2y - 1 \equiv 0 \pmod{8} \text{ and } \left(\frac{p}{q}\right) = -1 \text{ or } \left(\frac{x}{q}\right) = 1$$

$$p \equiv q \equiv 5 \pmod{8} \text{ and } (x + 2y - 1) \left(1 - \left(\frac{p}{q}\right)\right) / 2 \equiv 2 \left(1 + \left(\frac{x}{q}\right)\right) \pmod{8}$$

(2) *Let $q \equiv \pm 1 \pmod{8}$ and $\left(\frac{p}{q}\right) = 1$. Then $d_1 = (-1)^{1+(p-1)/2} 4p$ and $d_2 = (-1)^{(q-1)/2} q$ define a decomposition of d which is of the third kind, if and only if one of the following conditions is satisfied:*

$$q \equiv 1 \pmod{8}, (x + 2y - 1)(1 - \chi(-p)) \equiv 2(1 - \text{sgn}(x))\chi(p) \pmod{8} \text{ and } \left(\frac{x}{q}\right) = 1$$

$$p \equiv -1 \pmod{4}, q \equiv -1 \pmod{8} \text{ and } x + 2y - 1 \equiv 2 \left(1 - \left(\frac{x}{q}\right)\right) \chi(p) \pmod{8}$$

Herein $\chi(n)$ is equal to 1 or 0 according to $n \equiv 3 \pmod{8}$ or not.

PROOF. (1) Let $\mathfrak{p}$ and $\mathfrak{q}$ be the prime ideal of $Q(\sqrt{-4})$ dividing respectively p and q such that α is prime both to $\mathfrak{p}$ and to $\mathfrak{q}$. It follows from Lemma 2 that α (resp. $p\alpha$) is a quadratic residue modulo $\mathfrak{q}^5$ if and only if

$$x \equiv 1 - y^2 \pmod{8} \quad (\text{resp. } x \equiv p - y^2 \pmod{8}),$$

and it also follows from Lemma 3 that α (resp. $p\alpha$) is a quadratic residue modulo q if and only if

$$\left(\frac{x}{q}\right) = \left(\frac{2}{q}\right) \quad \left(\text{resp. } \left(\frac{px}{q}\right) = \left(\frac{2}{q}\right)\right),$$

and besides α (resp. $q\alpha$) is a quadratic residue modulo p if and only if

$$\left(\frac{x}{p}\right) = \left(\frac{2}{p}\right) \quad \left(\text{resp. } \left(\frac{qx}{p}\right) = \left(\frac{2}{p}\right)\right).$$

On the other hand, from (1) of Lemma 4, we always have $\left(\frac{x}{p}\right) = \left(\frac{x}{q}\right)$. And in this case y must be even, as easily deduced from the condition for α . Hence it follows from (3) of Proposition 2 that $d = d_1 d_2$ is a decomposition of the third kind, if and only if

$$x \equiv 1 - 2y \pmod{8} \text{ and } \left(\frac{x}{q}\right) = \left(\frac{2}{q}\right),$$

or

$$x \equiv p - 2y \pmod{8} \text{ and } \left(\frac{px}{q}\right) = \left(\frac{2}{q}\right).$$

This part of the theorem immediately follows from this.

(2) Let $\mathfrak{p}$ be the prime ideal of $Q(\sqrt{d_1})$ dividing p , and also $\mathfrak{q}$ the prime ideal of $Q(\sqrt{d_1})$ dividing q such that α is prime to $\mathfrak{q}$. It follows from Lemma 2 that α (resp. $(-1)^{(p-1)/2} p\alpha$) is a quadratic residue modulo $\mathfrak{q}^5$ if and only if

$$x \equiv 1 - (-1)^{\frac{p-1}{2}} p y^2 \pmod{8} \quad (\text{resp. } x \equiv (-1)^{\frac{p-1}{2}} p(1 - y^2) \pmod{8}),$$

and it also follows from Lemma 3 that α (resp. -4α) is a quadratic residue modulo p if and only if

$$\left(\frac{x}{p}\right) = 1 \quad \left(\text{resp. } \left(\frac{-4x}{p}\right) = 1\right),$$

and besides α (resp. -4α) is a quadratic residue modulo q if and only if

$$\left(\frac{x}{q}\right)=\left(\frac{2}{q}\right)=1 \quad \left(\text{resp. } \left(\frac{-4x}{q}\right)=\left(\frac{2}{q}\right)=1\right).$$

On the other hand, from (4) of Lemma 4, in the case $d < 0$ we always have $\left(\frac{x}{p}\right)=\left(\frac{x}{q}\right)$, and in the case $d > 0$ we have $\left(\frac{x}{p}\right)=\left(\frac{x}{q}\right)$ if and only if $x > 0$. And y must be also even. Hence it follows from (3) of Proposition 2 that $d = d_1 d_2$ is a decomposition of the third kind, if and only if in the case $d < 0$

$$x \equiv 1 - 2y \pmod{8} \text{ and } \left(\frac{x}{q}\right)=1,$$

or

$$x \equiv (-1)^{\frac{p-1}{2}} p - 2y \pmod{8} \text{ and } \left(\frac{x}{q}\right)=\left(\frac{-1}{q}\right),$$

and in the case $d > 0$,

$$x \equiv 1 - 2y \pmod{8}, x > 0 \text{ and } \left(\frac{x}{q}\right)=1,$$

or

$$x \equiv -p - 2y \pmod{8}, x < 0 \text{ and } \left(\frac{x}{q}\right)=1.$$

Then the theorem immediately follows from these.

4. The case where d is a multiple of 8

Finally, we shall consider the case where d is a multiple of 8: $d = \pm 8pq$. In this case it follows from (1) of Proposition 2 that $r_2 \geq 1$ if and only if at least one of the following conditions is satisfied:

$$p \equiv q \equiv 1, 3 \pmod{8} \quad (d_1 = -8, d_2 = pq)$$

$$p, q \equiv \pm 1 \pmod{8} \quad (d_1 = 8, d_2 = \pm pq)$$

$$q \equiv 1 \pmod{8} \text{ and } \left(\frac{p}{q}\right)=1 \quad (d_1 = -8p, d_2 = q)$$

$$q \equiv \pm 1 \pmod{8} \text{ and } \left(\frac{p}{q}\right) = 1 \quad (d_1 = 8p, d_2 = \pm q)$$

In particular, $r_2 = 2$ if and only if $p \equiv \pm q \equiv 1 \pmod{8}$ and $\left(\frac{p}{q}\right) = 1$.

We have then the following theorem. It is also proved from Lemmas 3 and 4 and Proposition 2 in a method similar to the proof of Theorem 1, and hence we give it without proof.

THEOREM 2. (1) *Let $p \equiv q \equiv 1, 3 \pmod{8}$. Then $d_1 = -8$ and $d_2 = pq$ define a decomposition of d which is of the third kind, if and only if one of the following conditions is satisfied:*

$$p \equiv q \equiv 1 \pmod{8}, x + 2y^2 - 1 \equiv 0 \pmod{8} \text{ and } \left(\frac{p}{q}\right) = -1 \text{ or } \left(\frac{x}{q}\right) = 1$$

$$p \equiv q \equiv 3 \pmod{8} \text{ and } (x + 2y^2 - 1)\left(1 + \left(\frac{p}{q}\right)\right)/2 \equiv 2\left(1 + \left(\frac{x}{q}\right)\right) \pmod{8}$$

(2) *Let $p \equiv \pm q \equiv 1 \pmod{8}$ or $p \equiv q \equiv -1 \pmod{8}$. Then $d_1 = 8$ and $d_2 = (-1)^{(p+q-1)/2}pq$ define a decomposition of d which is of the third kind, if and only if*

$$x - 2y^2 - 1 \equiv 0 \pmod{8}$$

and one of the following conditions are satisfied:

$$p \equiv \pm q \equiv 1 \pmod{8}, (1 - \text{sgn}(x))(1 + (-1)^{\frac{q-1}{2}}) = 0 \text{ and } \left(\frac{p}{q}\right) = -1 \text{ or } \left(\frac{x}{q}\right) = 1$$

$$p \equiv q \equiv -1 \pmod{8} \text{ and } \left(\frac{p}{q}\right) = -\left(\frac{x}{q}\right) = -1$$

(3) *Let $q \equiv 1 \pmod{8}$ and $\left(\frac{p}{q}\right) = 1$. Then $d_1 = -8p$ and $d_2 = q$ define a decomposition of d which is of the third kind, if and only if*

$$(x + 2py^2 - 1)(1 + (-1)^{\frac{p^2-1}{8}})/2 \equiv 0 \pmod{8} \text{ and } \left(\frac{x}{q}\right) = 1.$$

(4) *Let $q \equiv \pm 1 \pmod{8}$ and $\left(\frac{p}{q}\right) = 1$. Then $d_1 = 8p$ and $d_2 = (-1)^{(q-1)/2}q$ define a decomposition of d which is of the third kind, if and only if one of the following conditions is satisfied:*

$$\begin{aligned}
& p \equiv 1 \pmod{8}, x - 2y^2 - 1 \equiv 0 \pmod{8}, (1 - \operatorname{sgn}(x))(1 + (-1)^{\frac{q-1}{2}}) = 0 \\
& \qquad \qquad \qquad \text{and } \left(\frac{x}{q}\right) = 1 \\
& p \not\equiv 1 \pmod{8}, q \equiv 1 \pmod{8}, (x - 2py^2 - 1)(1 - (-1)^{\frac{p-1}{2}})/2 \\
& \qquad \qquad \qquad \equiv (1 - \operatorname{sgn}(x))(1 - (-1)^{\frac{p^2-1}{8}}) \pmod{8} \text{ and } \left(\frac{x}{q}\right) = 1 \\
& p \not\equiv 1 \pmod{8}, q \equiv -1 \pmod{8} \text{ and } (x + 2y^2 - 1)(1 - (-1)^{\frac{p-1}{2}})/2 \\
& \qquad \qquad \qquad \equiv \left(1 - \left(\frac{x}{q}\right)\right)(1 - (-1)^{\frac{p^2-1}{8}}) \pmod{8}
\end{aligned}$$

References

- [1] H. HASSE, *Über die Teilbarkeit durch 2^3 der Klassenzahl imaginär-quadratische Zahlkörper mit genau zwei verschiedenen Diskriminantenprimteilern*. J. Reine Angew. Math. **241** (1970), 1-6.
- [2] H. HASSE, *Über die Teilbarkeit durch 2^3 der Klassenzahl quadratischen Zahlkörper mit genau zwei verschiedenen Diskriminantenprimteilern*. Math. Nachr. **46** (1970), 61-70.
- [3] L. RÉDEI und H. REICHARDT, *Die Anzahl der durch 4 teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers*. J. Reine Angew. Math. **170** (1934), 69-74.
- [4] H. REICHARDT, *Zur Struktur der absoluten Idealklassengruppe im quadratischen Zahlkörper*. J. Reine Angew. Math. **170** (1934), 75-82.
- [5] H. REICHARDT, *Über die 2-Klassengruppe gewisser quadratischer Zahlkörper*. Math. Nachr. **46** (1970), 71-80.