M. Kutsuna
Nagoya Math. J.
Vol. 79 (1980), 123–129

# ON A CRITERION FOR THE CLASS NUMBER OF A QUADRATIC NUMBER FIELD TO BE ONE

MASAKAZU KUTSUNA

## § 0.

G. Rabinowitsch [3] generalized the concept of the Euclidean algorithm and proved a theorem on a criterion in order that the class number of an imaginary quadratic number field is equal to one:

THEOREM. *It is necessary and sufficient for the class number of an imaginary quadratic number field* $\boldsymbol{Q}(\sqrt{D})$, $D = 1 - 4m$, $m > 0$, *to be one that* $x^2 - x + m$ *is prime for any integer* $x$ *such that* $1 \leq x \leq m - 2$.

Rabinowitsch mentions there nothing on the case of real quadratic number fields. So, we shall give a similar result by applying his method to real quadratic number fields (Theorem 2, Cor. 1).

In § 1, we shall define *störend* fractions and give a criterion for the class number of a real quadratic number field to be one (Theorem 2). In § 2, we shall treat real quadratic number fields whose genus number is equal to one and give a table of such real quadratic number fields together with the effect of our criterion.

Notations. We denote by Latin letters $a, b, c, \cdots$, rational integers and by Greek letters $\alpha, \beta, \gamma, \cdots$, integers of a real quadratic field $K = \boldsymbol{Q}(\sqrt{D})$ where $D$ is a positive rational square-free integer. $\mathcal{O}_K$ is the ring of integers of $K$.

## § 1.

At first we give the following necessary and sufficient condition for the class number of $K$ to be one:

THEOREM 1. *It is a necessary and sufficient condition for the class number of* $K$ *to be one that for any integers* $\alpha, \beta$ *of* $K$, $(\alpha/\beta, \beta/\alpha \notin \mathcal{O}_K)$, *there exist two integers* $\xi, \eta$ *of* $K$ *such that*

Received March 20, 1979.

$$0 < |N(\alpha\xi - \beta\eta)| < |N\beta| . \tag{1}$$

For the proof of Theorem 1, we need the following

LEMMA 1. *If the class number of $K$ is bigger than one, there exist an indecomposable integer $\pi$ and an integer $\alpha$ of $K$ such that*

$$\alpha = \alpha_1\alpha_2,\ \pi|\alpha,\ \pi\nmid\alpha_i,\ \alpha_i \in \mathcal{O}_K , \qquad (i = 1, 2) . \tag{2}$$

*Proof.* If the class number of $K$ is bigger than one, there is an integer $\alpha$ of $K$ such that

$$\alpha = \pi_1\pi_2 \cdots \pi_k = \sigma_1\sigma_2 \cdots \sigma_\ell ,$$

where $\pi_i$, $(1 \leq i \leq k)$, and $\sigma_j$, $(1 \leq j \leq \ell)$, are distinct and indecomposable integers. Put $\pi = \pi_1$, then $\pi\nmid\sigma_j$, $(1 \leq j \leq \ell)$. Therefore, if $\pi\nmid\sigma_2 \cdots \sigma_\ell$, then $\alpha_1 = \sigma_1$ and $\alpha_2 = \sigma_2 \cdots \sigma_\ell$ satisfy (2). If $\pi|\sigma_2 \cdots \sigma_\ell$, then there exists a natural number $m$, $(2 \leq m \leq \ell - 1)$, such that $\pi|\sigma_m\sigma_{m+1} \cdots \sigma_\ell$ and $\pi\nmid\sigma_{m+1} \cdots \sigma_\ell$. Then $\alpha_1 = \sigma_m$ and $\alpha_2 = \sigma_{m+1} \cdots \sigma_\ell$ satisfy (2).

*Proof of Theorem* 1. Sufficiency: Suppose that the class number of $K$ is bigger than one. By Lemma 1, there exist an indecomposable integer $\pi$ and an integer $\alpha$ of $K$ which satisfies (2). Let $\alpha = \lambda\Lambda$ be the integer such that the norm is the smallest among those integers satisfying (2) where $\pi$ is fixed. By the assumption of Theorem 1, there exist two integers $\xi$ and $\eta$ of $K$ such that

$$|N(\pi\xi - \lambda\eta)| < |N\pi| , \qquad |N(\pi\xi - \lambda\eta)| < |N\lambda| .$$

Here, put $\mu = \pi\xi - \lambda\eta$, then $\pi|\mu\Lambda$, $\pi\nmid\mu$, $\pi\nmid\Lambda$ and $|N(\mu\Lambda)| < |N(\lambda\Lambda)|$. This is a contradiction.

Necessity: Let $\alpha, \beta$ be two integers of $K$ such that $\alpha/\beta \notin \mathcal{O}_K$, $\beta/\alpha \notin \mathcal{O}_K$. Here, we consider two ideals $(\alpha)$ and $(\beta)$. Put $(\gamma) = (\alpha, \beta)$, then $(\alpha) = (\gamma)(\alpha_0)$, $(\beta) = (\gamma)(\beta_0)$ and $(\alpha_0, \beta_0) = 1$. There exist integers $\xi$ and $\eta$ of $K$ such that $\alpha_0\xi - \beta_0\eta = 1$. Then we have

$$|N(\alpha\xi - \beta\eta)| = |N\gamma| < |N\beta| .$$

DEFINITION. Let $\alpha/\beta$ be any fraction in $K$ such that $\alpha/\beta \notin \mathcal{O}_K$ and $\beta/\alpha \notin \mathcal{O}_K$. Then, we call $\alpha/\beta$ *störend* if there exist no integers $\xi, \eta$ of $K$ such that $0 < |N(\alpha/\beta \cdot \xi - \eta)| < 1$.

According to this definition, Theorem 1 is also expressed as follows:

https://doi.org/10.1017/S0027763000018961 Published online by Cambridge University Press

THEOREM 1′. *It is a necessary and sufficient condition for the class number of $K$ to be one that there exist no störend fractions in $K$.*

LEMMA 2. 1°. *If $\alpha/\beta$ is störend, then for any integer $\xi$ of $K$, $\alpha/\beta + \xi$ and $\alpha/\beta \cdot \xi$ ($\notin \mathcal{O}_K$) are also störend.*
2°. *Any rational fraction $a/b$ ($\notin \boldsymbol{Z}$) is not störend.*

*Proof.* 1° is obvious by the definition.
To prove 2°, put $a = bq + r$, $0 < r < b$. Then we have

$$0 < N(a/b - q) = r^2/b^2 < 1 .$$

PROPOSITION 1. *If the class number of $K$ is not equal to one, then there exists a störend fraction $(a - \vartheta)/p$ such that $0 \leq a < p$, where $p$ is a rational prime and*

$$\vartheta = \begin{cases} \dfrac{1 + \sqrt{D}}{2} & (D \equiv 1 \bmod 4) , \\ \sqrt{D} & (D \equiv 2, 3 \bmod 4) . \end{cases}$$

*Proof.* If the class number of $K$ is not equal to one, then by Theorem 1′ there is a störend fraction $\alpha/\beta$ in $K$. Here, we rationalize the denominator of $\alpha/\beta$. Then we have a störend fraction $(A + C\vartheta)/p$, where $A, C, p \in \boldsymbol{Z}$, $(A, C, p) = 1$ and $p$ is a rational prime, by Lemma 2. Furthermore we can take $C$ such that $(C, p) = 1$. Therefore, there exist two rational integers $x$ and $y$ such that $Cx - py = -1$. Hence $(A + C\vartheta)/p \cdot x - y\vartheta = (Ax - \vartheta)/p$ is a störend fraction by Lemma 2. Let $a$ be a rational integer such that $Ax \equiv a \pmod{p}$ and $0 \leq a < p$, then $(a - \vartheta)/p$ is a desired fraction.

Hereafter we put $D = 1 + 4m$ when $D \equiv 1 \pmod 4$.

PROPOSITION 2. *If a fraction $(a - \vartheta)/p$ is störend and $0 \leq a < p$, then we have*

$$p \leq \begin{cases} \sqrt{m} & (D \equiv 1 \bmod 4) , \\ \sqrt{D} & (D \equiv 2, 3 \bmod 4) . \end{cases}$$

*Proof.* Since the absolute value of the norm of any störend fraction is not smaller than one, we have

$$p^2 \leq |N(a - \vartheta)| = \begin{cases} |a^2 - a - m| & (D \equiv 1 \bmod 4) , \\ |a^2 - D| & (D \equiv 2, 3 \bmod 4) . \end{cases}$$

Hence

https://doi.org/10.1017/S0027763000018961 Published online by Cambridge University Press

$$p^2 \leq \begin{cases} -a + a + m \leq m & (D \equiv 1 \bmod 4)\,, \\ -a + D \leq D & (D \equiv 2, 3 \bmod 4)\,, \end{cases}$$

since $0 \leq a < p$.

Proposition 1 is modified by Proposition 2 as follows:

PROPOSITION 3. *If the class number of $K$ is bigger than one, then there exists a störend fraction $(a - \vartheta)/p$ such that $p$ is a rational prime and*

$$0 \leq a < p \leq \begin{cases} \sqrt{m} & (D \equiv 1 \bmod 4)\,, \\ \sqrt{D} & (D \equiv 2, 3 \bmod 4)\,. \end{cases}$$

We next consider the condition for a fraction $(a - \vartheta)/p$ of $K$ not to be störend.

PROPOSITION 4. *If $N(a - \vartheta)$ is relatively prime to $p$ or if there exists a rational integer $k$ such that $|N(a + kp - \vartheta)| < p^2$, then $(a - \vartheta)/p$ is not störend.*

*Proof.* If $N(a - \vartheta)$ is relatively prime to $p$, then there exist rational integers $x$ and $y$ such that $N(a - \vartheta) \cdot x - yp = 1$. Then we have

$$\frac{a - \vartheta}{p} \cdot (a - \bar{\vartheta})x - y = \frac{1}{p}\,,$$

where $\bar{\vartheta}$ denotes the conjugate of $\vartheta$ in $K$. Hence, $(a - \vartheta)/p$ is not störend by Lemma 2.

If $|N(a + kp - \vartheta)| < p^2$, then $(a + kp - \vartheta)/p$ is not störend. Therefore $(a - \vartheta)/p$ is not störend.

From Proposition 3 and Proposition 4, we obtain immediately a criterion for the class number of a quadratic field $K = \boldsymbol{Q}(\sqrt{D})$ to be one:

THEOREM 2. *Case* 1. $D \equiv 1 \pmod 4$, $(D = 1 + 4m)$.
*If, for any given rational prime $p$ such that $1 < p \leq \sqrt{m}$ and for any given rational integer $a$ such that $0 \leq a < p$, either $N(a - \vartheta)$ is relatively prime to $p$ or there exists a rational integer $k$ such that $|N(a + kp - \vartheta)| < p^2$, then there exists no störend fraction in $K$, and hence the class number of $K$ is equal to one.*

*Case* 2. $D \equiv 2, 3 \pmod 4$.
*If, for any given rational prime $p$ such that $1 < p < \sqrt{D}$ and for any given rational integer $a$ such that $0 \leq a < p$, either $N(a - \vartheta)$ is relatively prime to $p$ or there exists a rational integer $k$ such that $|N(a + kp - \vartheta)| < p^2$, then*

https://doi.org/10.1017/S0027763000018961 Published online by Cambridge University Press

*there exists no störend fraction in K, and hence the class number of K is equal to one.*

COROLLARY. *In case of* $D \equiv 1 \pmod 4$, $(D = 1 + 4m)$.
1°. *If* $-x^2 + x + m$ *is a rational prime for any rational integer* $x$ *such that* $1 \leq x \leq \sqrt{m} - 1$, *then the class number of* $\boldsymbol{Q}(\sqrt{D})$ *is equal to one.*
2°. *If* $m$ *is odd and if* $(D/\ell) = -1$ *for any rational prime* $\ell$ *such that* $2 < \ell \leq \sqrt{m}$, *then the class number of* $\boldsymbol{Q}(\sqrt{D})$ *is equal to one.*

*Proof.* 1° is trivial by Theorem 2, Proposition 3 and Proposition 4. 2° is proved as follows: If $p = 2$ then $a = 0, 1$ and $N(a - \vartheta) = m$ is relatively prime to $p$. If $p > 2$, then $(D/p) = -1$. On the other hand,

$$N(a - \vartheta) \equiv 0 \pmod p \Longleftrightarrow D \equiv (2a - 1)^2 \pmod p \Longleftrightarrow (D/p) \neq -1 .$$

Therefore $N(a - \vartheta)$ is relatively prime to $p$. Hence the class number of $\boldsymbol{Q}(\sqrt{D})$ is equal to one by Theorem 2.

*Remark.* There exist following nine values of $D$ smaller than 2,000 which satisfy the assumption of Cor. 1° or 2°:

$$D = 5,\ 13,\ 21,\ 29,\ 53,\ 77,\ 173,\ 293,\ 437 .$$

## § 2.

In this section we investigate a quadratic number field $\boldsymbol{Q}(\sqrt{D})$ whose genus number is one.

LEMMA 3. *Case* 1. $D \equiv 1 \pmod 4$, $(D = 1 + 4m)$.
*For any rational prime* $p$ *and any rational integer* $a$ *such that* $0 \leq a \leq (p - 1)/2$, $(a - \vartheta)/p$ *is störend if and only if* $(p + 1 - a - \vartheta)/p$ *is störend.*
*Case* 2. $D \equiv 2, 3 \pmod 4$.
*For any rational prime* $p$ *and for any rational integer* $a$ *such that* $1 \leq a \leq (p - 1)/2$, $(a - \vartheta)/p$ *is störend if and only if* $(p - a - \vartheta)/p$ *is störend.*

*Proof.* Case 1. Since $N(s + t\vartheta) = N(s + t - t\vartheta)$, we have

$$\begin{aligned} &N((a - \vartheta)/p \cdot (s + t\vartheta) + u + v\vartheta) \\ &\quad = N((p + 1 - a - \vartheta)/p \cdot (s + t - t\vartheta) - (s + t + u + v) + (t + v)\vartheta) . \end{aligned}$$

Therefore, lemma is obtained from Lemma 2.
Case 2. Since $N(s + t\vartheta) = N(-s + t\vartheta)$, we have

$$\begin{aligned} &N((a - \vartheta)/p \cdot (s + t\vartheta) + u + v\vartheta) \\ &\quad = N((p - a - \vartheta)/p \cdot (s + t\vartheta) - s - u + (t + v)\vartheta) . \end{aligned}$$

https://doi.org/10.1017/S0027763000018961 Published online by Cambridge University Press

Therefore, lemma is obtained from Lemma 2.

PROPOSITION 5. *Case* 1. $D = \ell \equiv 1 \pmod 4$ *prime*, $(D = 1 + 4m)$. *Let* $p$ *be any rational prime such that* $1 < p \leq \sqrt{m}$, *and suppose that fractions* $(a - \vartheta)/p$, $0 \leq a < p$, *are not störend except at most one. Then all of them are not störend.*

*Case* 2. $D = q$ *or* $2q$, $q \equiv 3 \pmod 4$ *prime.*
*Fractions* $(a - \vartheta)/2$, $a = 0, 1$, *are not störend. Let next* $p$ *be any rational prime such that* $2 < p \leq \sqrt{D}$, *and suppose that fractions* $(a - \vartheta)/p$, $0 \leq a < p$, *are not störend except at most one. Then all of them are not störend.*

*Proof.* Case 1. Since $p \leq \sqrt{m} < D$, we have $p \nmid D$ i.e. $(D/p) \neq 0$. Hence, if there exists a rational integer $a$ such that $N(a - \vartheta) \equiv 0 \pmod p$ and $0 \leq a < p$, then there exist two rational integers $a$ such that $N(a - \vartheta) \equiv 0 \pmod p$ and $0 \leq a < p$. From the assumption of Proposition 5 and Lemma 3, both of two fractions $(a - \vartheta)/p$ are not störend for such two values of $a$.

Case 2. In case of $p = 2$, it is well-known (Perron [2] p. 109) that the Diophantine equation $x^2 - Dy^2 = \pm 2$ is solvable when $D = q$ or $2q$ where $q$ is a rational prime such that $q \equiv 3 \pmod 4$. From this fact, it is easy to prove that fractions $(a - \vartheta)/2$, $a = 0, 1$, are not störend. In case of $p > 2$, lemma is proved similarly to Case 1.

Table 1

$K = Q(\sqrt{D})$, $D = \ell = 1 + 4m$ prime, $p$ prime s.t. $1 < p \leq \sqrt{m}$, $h$ class number of $K$ $(*)$ means the effect of the criterion (Theorem 2, Proposition 5) by 0

| $D$ | $m$ | $p$ | $-N(a - \vartheta) = -a^2 + a + m$ | | | | | | | | | $(*)$ | $h$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | $a=1$ | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | | |
| 5 | 1 | | | | | | | | | | | 0 | 1 |
| 13 | 3 | | | | | | | | | | | 0 | 1 |
| 17 | 4 | 2 | 4 | 2 | | | | | | | | 0 | 1 |
| 29 | 7 | 2 | 7 | | | | | | | | | 0 | 1 |
| 37 | 9 | 2, 3 | 9 | 7 | 3 | | | | | | | 0 | 1 |
| 41 | 10 | 2, 3 | 10 | 8 | 4 | −2 | | | | | | 0 | 1 |
| 53 | 13 | 2, 3 | 13 | 11 | | | | | | | | 0 | 1 |

Table 1 (continued)

| $D$ | $m$ | $p$ | $-N(a-\vartheta) = -a^2+a+m$ | | | | | | | | | (*) | $h$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 61 | 15 | 2, 3 | 15 | 13 | 9 | 3 | | | | | | 0 | 1 |
| 73 | 18 | 2, 3 | 18 | 16 | 12 | 6 | −2 | | | | | 0 | 1 |
| 89 | 22 | 2, 3 | 22 | 20 | 16 | 10 | 2 | | | | | 0 | 1 |
| 97 | 24 | 2, 3 | 24 | 22 | 18 | 12 | 4 | −6 | | | | | 1 |
| 101 | 25 | 2, 3, 5 | 25 | 23 | 19 | 13 | 5 | | | | | 0 | 1 |
| 109 | 27 | 2, 3, 5 | 27 | 25 | 21 | 15 | 7 | −3 | | | | 0 | 1 |
| 113 | 28 | 2, 3, 5 | 28 | 26 | 22 | 16 | 8 | −2 | | | | 0 | 1 |
| 137 | 34 | 2, 3, 5 | 34 | 32 | 28 | 22 | 14 | 4 | | | | | 1 |
| 149 | 37 | 2, 3, 5 | 37 | 35 | 31 | 25 | 17 | 7 | −5 | | | 0 | 1 |
| 157 | 39 | 2, 3, 5 | 39 | 37 | 33 | 27 | 19 | 9 | −3 | | | 0 | 1 |
| 161 | 40 | 2, 3, 5 | 40 | 38 | 34 | 28 | 20 | 10 | −2 | | | 0 | 1 |
| 173 | 43 | 2, 3, 5 | 43 | 41 | 37 | 31 | | | | | | 0 | 1 |
| 193 | 48 | 2, 3, 5 | 48 | 46 | 42 | 36 | 28 | 18 | 6 | −8 | | | 1 |
| 197 | 49 | 2, 3, 5, 7 | 49 | 47 | 43 | 37 | 29 | 19 | 7 | | | 0 | 1 |
| 229 | 57 | 2, 3, 5, 7 | 57 | 55 | 51 | 45 | 37 | 27 | 15 | 1 | −15 | | 3 |
| 233 | 58 | 2, 3, 5, 7 | 58 | 56 | 52 | 46 | 38 | 28 | 16 | 2 | −14 | 0 | 1 |
| 241 | 60 | 2, 3, 5, 7 | 60 | 58 | 54 | 48 | 40 | 30 | 18 | 4 | −12 | | 1 |
| 257 | 64 | 2, 3, 5, 7 | 64 | 62 | 58 | 52 | 44 | 34 | 22 | 8 | −8 | | 3 |

## References

[1] Nagel, T., Über die Klassenzahl imaginär-quadratischer Zahlkörper. Abh. Math. Sem. U. Hamburg **1** (1922), 140–150.

[2] Perron, O., Die Lehre von den Kettenbrüchen, 2. Auf. Chelsea.

[3] Rabinowitsch, G., Eindeutigkeit der Zerlegung in Primzahlfaktoren in quadratischen Zahlkörpern. J. reine angew. Math. **142** (1913), 153–164.

*Department of Liberal Arts,*
*Gifu Technical College*