

**ON THE DIOPHANTINE EQUATION $x^2 - py^2 = \pm 4q$ AND
THE CLASS NUMBER OF REAL SUBFIELDS
OF A CYCLOTOMIC FIELD***

HIDEO YOKOI

Introduction

Let $H(m)$ denote the class number of the field $K = \mathbf{Q}(\zeta_m + \zeta_m^{-1})$, where \mathbf{Q} is the rational number field and ζ_m is a primitive m -th root of unity for a positive rational integer m .

It has been proved by Ankeny, Chowla and Hasse in [2] that if $p = (2nq)^2 + 1$ is a prime, with prime q and integer $n > 1$, then $H(p) > 1$. Later, S.-D. Lang proved in [5] that if $p = ((2n + 1)q)^2 + 4$ is a prime, with odd prime q and integer $n \geq 1$, then $H(p) > 1$.

Both results are based on the fact that the diophantine equation $x^2 - py^2 = \pm 4m$ has no solution (x, y) in integers unless $m \geq nq$ (resp. $m \geq (2n + 1)q$).

In this paper, we shall first consider the diophantine equation $x^2 - py^2 = \pm 4q$ for distinct odd primes p, q , and give a necessary and sufficient condition for its solvability (§ 1). Next, we shall show that for distinct odd primes p, q satisfying $p = ((2n + 1)q)^2 \pm 2$ with integer $n \geq 0$ the diophantine equation $x^2 - py^2 = \pm q$ has no solution (x, y) in integers except for the case $p = 7$ ($n = 0, q = 3$) (§ 2).

Moreover, in Section 3, for a prime p of such type, we shall give a sufficient condition for the class number $h(p)$ of the real quadratic field $\mathbf{Q}(\sqrt{p})$ to be greater than 1, and by applying this result to maximal real subfield of a cyclotomic field we shall also give a sufficient condition for $H(4p) > 1$.

Finally, we shall list up all primes $p < 100,000$ satisfying $p = ((2n + 1)q)^2 - 2$ with prime $q \equiv 1$ or $3 \pmod{4}$, ($n \geq 0$), and $p = ((2n + 1)q)^2 + 2$ with prime $q \equiv 1$ or $7 \pmod{4}$, ($n \geq 0$), for which both $h(p)$ and $H(4p)$ are

* This research was partially supported by Grant-in-Aid for Scientific Research Project No. 56540017, Ministry of Education, Japan.

greater than 1.

§ 1. Solvability of the equation $x^2 - py^2 = \pm 4q$

We consider, in this section, the diophantine equation $x^2 - py^2 = \pm 4q$ for distinct odd primes p, q . However, the following fact is noteworthy: When the equation $x^2 - py^2 = \pm q$ has a solution (u, v) in integers, the double of the solution $(2u, 2v)$ is also a solution of the equation $x^2 - py^2 = \pm 4q$. Conversely, in the case $p \not\equiv 1 \pmod{4}$ all the solutions of $x^2 - py^2 = \pm 4q$ can be obtained from the solutions $x^2 - py^2 = \pm q$ in such a way, while in the case $p \equiv 1 \pmod{4}$ not all the solutions can necessarily be found from the solutions of $x^2 - py^2 = \pm q$.

The following fact, which gives a relation between the solvability of the equation $x^2 - py^2 = \pm 4q$ and the class number of the real quadratic field $\mathbf{Q}(\sqrt{p})$, is already known¹⁾, but is fundamental in our investigation. Therefore, we state it as a theorem and, for the sake of completeness, add a simple proof:

THEOREM 1. *Let p and q be two distinct odd primes. Then, the diophantine equation $x^2 - py^2 = \pm 4q$ has at least one solution (x, y) in integers if and only if the prime q splits completely in the real quadratic field $\mathbf{Q}(\sqrt{p})$ into the product of a principal prime ideal \mathfrak{q} with degree one and its conjugate \mathfrak{q}' : $q = \mathfrak{q} \cdot \mathfrak{q}'$, ($\mathfrak{q} \neq \mathfrak{q}'$, $N\mathfrak{q} = N\mathfrak{q}' = q$, $\mathfrak{q} = (\omega)$, $\mathfrak{q}' = (\omega')$ with ω, ω' in $\mathbf{Q}(\sqrt{p})$).*

Proof. If there exists one solution (u, v) in integers of $x^2 - py^2 = \pm 4q$, then $u^2 - pv^2 = \pm 4q$ implies $u^2 \equiv pv^2 \pmod{q}$. Hence $1 = (pv^2/q) = (p/q)$ holds, and so by the law of decomposition in quadratic fields q splits completely in $\mathbf{Q}(\sqrt{p})$. On the other hand, it follows from $\pm q = (u + v\sqrt{p})/2 \cdot (u - v\sqrt{p})/2$ that both

$$\mathfrak{q} = \left(\frac{u + v\sqrt{p}}{2} \right) \quad \text{and} \quad \mathfrak{q}' = \left(\frac{u - v\sqrt{p}}{2} \right)$$

are principal ideals in $\mathbf{Q}(\sqrt{p})$ and $N\mathfrak{q} = \mathfrak{q} \cdot \mathfrak{q}' = q$ holds. Therefore \mathfrak{q} and \mathfrak{q}' are principal prime ideals in $\mathbf{Q}(\sqrt{p})$ with degree one.

Conversely, if q splits completely in $\mathbf{Q}(\sqrt{p})$ into the product of two principal prime ideals $\mathfrak{q}, \mathfrak{q}'$ with degree one, then there exist two rational

1) Cf. e. g. [2], [3] etc.

integers u, v such that both $\omega = (u + v\sqrt{p})/2$ and $\omega' = (u - v\sqrt{p})/2$ are integers in $\mathbf{Q}(\sqrt{p})$ and $\mathfrak{q} = (\omega)$, $\mathfrak{q}' = (\omega')$. Hence

$$q = \mathfrak{q} \cdot \mathfrak{q}' = N\mathfrak{q} = |N(\omega)| = \left| \frac{u^2 - pv^2}{4} \right|$$

implies $u^2 - pv^2 = \pm 4q$. Therefore $x^2 - py^2 = \pm 4q$ has the solution (u, v) in integers, which completes the proof of Theorem 1.

For example, let p and q be two odd primes satisfying $p = 4q^2 + 1$ or $p = q^2 + 4$. Then, the equation $x^2 - py^2 = \pm 4q$ has a solution $(2q \pm 1, 1)$ or $(q \pm 2, 1)$ in integers respectively. On the other hand, the prime q splits completely in $\mathbf{Q}(\sqrt{p})$ such as

$$q = \mathfrak{q} \cdot \mathfrak{q}'; \quad \mathfrak{q} = \left(\frac{2q \pm 1 + \sqrt{p}}{2} \right), \quad \mathfrak{q}' = \left(\frac{2q \pm 1 - \sqrt{p}}{2} \right)$$

or

$$\mathfrak{q} = \left(\frac{q \pm 2 + \sqrt{p}}{2} \right), \quad \mathfrak{q}' = \left(\frac{q \pm 2 - \sqrt{p}}{2} \right)$$

respectively.

From Theorem 1 we deduce easily:

COROLLARY. *Let p and q be two odd primes satisfying $p = (nq)^2 + r^2$ for natural numbers n, r . Then, the class number $h(p)$ of the real quadratic field $\mathbf{Q}(\sqrt{p})$ is not equal to one i.e. $h(p) > 1$ if $x^2 - py^2 = \pm 4q$ has no solution (x, y) in integers.*

Proof. Since the condition $p = (nq)^2 + r^2$ implies immediately $(p/q) = 1$, prime q splits completely in $\mathbf{Q}(\sqrt{p})$. Hence, if we suppose $h(p) = 1$, then it follows from Theorem 1 that $x^2 - py^2 = \pm 4q$ has at least one solution (x, y) in integers. This is a contradiction. Therefore $h(p) = 1$ is impossible, which proves the assertion of Corollary.

§ 2. Solvability of the equation $x^2 - py^2 = \pm q$ for $p = ((2n + 1)q)^2 \pm 2$

After Ankeny-Chowla-Hasse and S.-D. Lang, H. Takeuchi proved in [6] that if both $12m + 7$ and $p = (3(8m + 5))^2 - 2$ are primes or both $12m + 11$ and $p = (3(8m + 7))^2 - 2$ are primes with an integer $m \geq 0$, then the equation $x^2 - py^2 = \pm 3$ has no solution (x, y) in integers.

Here, we prove more generally:

THEOREM 2. *Let p and q be two odd primes satisfying $p = ((2n + 1)q)^2$*

± 2 with an integer $n \geq 0$, Then, the diophantine equation $x^2 - py^2 = \pm q$ has at least one solution (x, y) in integers if and only if $p = 7$ and $q = 3$ ($n = 0$) i.e. only the equation $x^2 - 7y^2 = -3$ has a solution in integers, for example $(x, y) = (2, 1)$.

Proof. (1) Let p and q be two odd primes satisfying $p = ((2n + 1)q)^2 - 2$ with an integer $n \geq 0$, and put $l = (2n + 1)q$.

Assume first that $x^2 - py^2 = q$ has at least one solution in integers, and let (u, v) ($u > 0, v > 0$) be the least such positive integral solution: $u^2 - pv^2 = q$.

In the case $q > 2v^2$, where $q = u^2 - pv^2 = u^2 - l^2v^2 + 2v^2$ implies easily $(u - lv)(u + lv) = q - 2v^2 > 0$, both $a = u - lv > 0$ and $b = u + lv > 0$ are positive rational integers, and $l = (b - a)/2v$, $q = ab + 2v^2$ holds. On the other hand, since $a \geq 1, b \geq 1$ and $(a - 1)(b + 1) = ab + a - b - 1$, we know $ab - 1 \geq b - a$. Therefore

$$\begin{aligned} 0 \leq 2nq = l - q &= \frac{b - a}{2v} - ab - 2v^2 = \frac{1}{2v} (b - a - 2vab - 4v^3) \\ &\leq \frac{1}{2v} (ab - 1 - 2vab - 4v^3) = \frac{-1}{2v} ((4v^3 + 1) + (2v - 1)ab) < 0. \end{aligned}$$

It is clear that this is a contradiction.

In the case $q < 2v^2$, the norm form $1 = N\varepsilon = N((l^2 - 1) + l\sqrt{l^2 - 2})$ of the fundamental unit²⁾ $\varepsilon = (l^2 - 1) + l\sqrt{l^2 - 2}$ of $\mathbf{Q}(\sqrt{p})$ multiplied by the norm form $q = N(u - v\sqrt{l^2 - 2})$ of $u^2 - pv^2 = q$ yields

$$\begin{aligned} q &= N[\{(l^2 - 1)u - lv(l^2 - 2)\} + \{lu - (l^2 - 1)v\}\sqrt{l^2 - 2}] \\ &= \{(l^2 - 1)u - lv(l^2 - 2)\}^2 - (l^2 - 2)\{lu - (l^2 - 1)v\}^2. \end{aligned}$$

Because of the minimal choice of v , we have $|lu - (l^2 - 1)v| \geq v$. Here, if $lu - (l^2 - 1)v \geq v$ i.e. $u \geq lv$, we have

$$q = u^2 - (l^2 - 2)v^2 \geq l^2v^2 - (l^2 - 2)v^2 = 2v^2,$$

which contradicts $q < 2v^2$. If $(l^2 - 1)v - lu \geq v$ i.e. $(l^2 - 2)v \geq lu$, we have

$$l^2q = l^2u^2 - l^2(l^2 - 2)v^2 \leq (l^2 - 2)^2v^2 - l^2(l^2 - 2)v^2 = -2(l^2 - 2)v^2 < 0,$$

which is also a contradiction.

2) Cf. [1], [3].

Therefore, it is impossible that for the prime $p = ((2n + 1)q)^2 - 2$ the equation $x^2 - py^2 = q$ has a solution in integers.

Next, assume that $x^2 - py^2 = -q$ has at least one solution in integers, and let (u, v) ($u > 0, v > 0$) be the least such positive integral solution: $u^2 - pv^2 = -q$.

In the case $q = 3, v = 1$, where $-3 = -q = u^2 - pv^2 = u^2 - l^2 + 2$ implies $(l - u)(l + u) = 5$, we have $l - u = 1, l + u = 5$, and so $l = 3, u = 2, p = 7$ is only one possible case as asserted in the Theorem.

In the case $q = 3, v \geq 2$ or $q > 3, v \geq q$, the norm form of the fundamental unit ε of $Q(\sqrt{p})$ multiplied by the norm form $-q = N(u - v\sqrt{l^2 - 2})$ of the equation $u^2 - pv^2 = -q$, together with the minimal choice of v , yields $|lu - (l^2 - 1)v| \geq v$. Here, if $lu - (l^2 - 1)v \geq v$, we have $-q = u^2 - (l^2 - 2)v^2 \geq l^2v^2 - (l^2 - 2)v^2 = 2v^2 > 0$, which is a contradiction. If $(l^2 - 1)v - lu \geq v$, we have

$$-l^2q = l^2u^2 - l^2(l^2 - 2)v^2 \leq (l^2 - 2)^2v^2 - l^2(l^2 - 2)v^2 = -2(l^2 - 2)v^2,$$

and hence $l^2q \geq 2(l^2 - 2)v^2$. Therefore, in the case of $q = 3$ and $v \geq 2$, $3l^2 \geq 2(l^2 - 2)v^2 \geq 8(l^2 - 2)$ implies $16 \geq 5l^2 \geq 45$, which is a contradiction. In the case of $v \geq q > 3$, $l^2v \geq l^2q \geq 2l^2v^2 - 4v^2$ implies $4v^2 \geq (2v^2 - v)l^2 \geq v(2v - 1)q^2$, and hence $q^2 \leq 4v/(2v - 1) = 2 + 2/(2v - 1) < 2 + 2/5 < 3$ holds. This is also a contradiction.

In the case $q > 3, v < q$, where $-q = u^2 - pv^2 = u^2 - l^2v^2 + 2v^2$ implies $(lv - u)(lv + u) = q + 2v^2 > 0$, both $a = lv - u > 0$ and $b = lv + u > 0$ are positive rational integers, and $l = (a + b)/2v, q = ab - 2v^2$. On the other hand, since $a \geq 1, b \geq 1$ and $(a - 1)(b - 1) = ab - (a + b) + 1$, we know $ab + 1 \geq a + b$. Therefore

$$\begin{aligned} 0 \leq 2nq = l - q &= \frac{a + b}{2v} - ab + 2v^2 = \frac{1}{2v}(a + b - 2vab + 4v^3) \\ &\leq \frac{1}{2v}(ab + 1 - 2vab + 4v^3) = \frac{1}{2v}((4v^3 + 1) - (2v - 1)ab) \end{aligned}$$

implies $4v^3 + 1 \geq (2v - 1)ab$, and so $ab \leq (4v^3 + 1)/(2v - 1)$. Hence

$$q = ab - 2v^2 \leq \frac{4v^3 + 1}{2v - 1} - 2v^2 = \frac{2v^2 + 1}{2v - 1} = v + \frac{v + 1}{2v - 1}.$$

Here, if $v = 1$ or 2 , then $q \leq v + (v + 1)/(2v - 1) = 3$, which is a contradiction. If $v \geq 3$, then $0 < (v + 1)/(2v - 1) < 1$ implies $q \leq v + (v + 1)/(2v - 1) < v + 1$, which contradicts $q > v$.

Therefore, it is impossible except for the case of $p = 7, q = 3$ ($n = 0$) that for $p = ((2n + 1)q)^2 - 2$ the equation $x^2 - py^2 = -q$ has a solution in integers.

(2) Let p and q be two odd primes satisfying $p = ((2n + 1)q)^2 + 2$ with an integer $n \geq 0$, and put $l = (2n + 1)q$.

Assume first that $x^2 - py^2 = q$ has at least one solution in integers, and let (u, v) ($u > 0, v > 0$) be the least such positive integral solution: $u^2 - pv^2 = q$.

In the case $q > v$, where $q = u^2 - l^2v^2 - 2v^2$ implies $(u - lv)(u + lv) = q + 2v^2 > 0$, both $a = u - lv > 0$ and $b = u + lv > 0$ are positive rational integers, and $l = (b - a)/2v, q = ab - 2v^2$ holds. Hence, we get

$$\begin{aligned} 0 \leq 2nq &= l - q = \frac{b - a}{2v} - (ab - 2v^2) = \frac{1}{2v}(b - a - 2vab + 4v^3) \\ &\leq \frac{1}{2v}(ab - 1 - 2vab + 4v^3) = \frac{1}{2v}((4v^3 - 1) - (2v - 1)ab), \end{aligned}$$

and so $ab \leq (4v^3 - 1)/(2v - 1)$. Therefore, we get

$$q = ab - 2v^2 \leq \frac{4v^3 - 1}{2v - 1} - 2v^2 = \frac{2v^2 - 1}{2v - 1} = v + \frac{v - 1}{2v - 1} < v + 1.$$

This, however, contradicts $q > v$.

In the case $q \leq v$, the norm form $1 = N\varepsilon = N((l^2 + 1) + l\sqrt{l^2 + 2})$ of the fundamental unit³⁾ $\varepsilon = (l^2 + 1) + l\sqrt{l^2 + 2}$ of $\mathbf{Q}(\sqrt{p})$ multiplied by the norm form $q = N(u - v\sqrt{l^2 + 2})$ of the equation $u^2 - pv^2 = q$, yields

$$q = \{u(l^2 + 1) - lv(l^2 + 2)\}^2 - (l^2 + 2)\{lu - (l^2 + 1)v\}^2.$$

Because of the minimum choice of v , we have $|lu - (l^2 + 1)v| \geq v$. Here, if $lu - (l^2 + 1)v \geq v$, we have

$$l^2q = l^2u^2 - l^2(l^2 + 2)v^2 \geq (l^2 + 2)^2v^2 - l^2(l^2 + 2)v^2 = 2(l^2 + 2)v^2 \geq 2(l^2 + 2)q^2,$$

and hence $q \leq l^2/2(l^2 + 2) < 1/2$. This is a contradiction. If $(l^2 + 1)v - lu \geq v$, we have $q = u^2 - (l^2 + 2)v^2 \leq l^2v^2 - (l^2 + 2)v^2 = -2v^2 < 0$. This is also a contradiction.

Assume next that $x^2 - py^2 = -q$ has at least one solution in integers, and let (u, v) ($u > 0, v > 0$) be the least such positive integral solution: $u^2 - pv^2 = -q$.

³⁾ Cf. [1], [3].

In the case $q > 2v^2$, where $-q = u^2 - l^2v^2 - 2v^2$ implies $(lv - u)(lv + u) = q - 2v^2 > 0$, both $a = lv - u > 0$ and $b = lv + u > 0$ are positive rational integers, and $l = (a + b)/2v$, $q = ab + 2v^2$ holds. Hence, we get

$$\begin{aligned} 0 \leq l - q &= \frac{a + b}{2v} - (ab + 2v^2) = \frac{1}{2v}(a + b - 2vab - 4v^3) \\ &\leq \frac{1}{2v}(ab + 1 - 2vab - 4v^3) = \frac{-1}{2v}((2v - 1)ab + (4v^3 - 1)) < 0. \end{aligned}$$

This is a contradiction.

In the case $q < 2v^2$, the norm form of the fundamental unit ϵ of $\mathbb{Q}(\sqrt{p})$ multiplied by the norm form $-q = N(u - v\sqrt{l^2 + 2})$ of the equation $u^2 - pv^2 = -q$, together with the minimal choice of v , yields $|lu - (l^2 + 1)v| \geq v$. Here, if $lu - (l^2 + 1)v \geq v$, we have

$$-l^2q = l^2u^2 - l^2(l^2 + 2)v^2 \geq (l^2 + 2)^2v^2 - l^2(l^2 + 2)v^2 = 2(l^2 + 2)v^2 = 2pv^2 > 0,$$

which is a contradiction. If $(l^2 + 1)v - lu \geq v$, we have

$$-q = u^2 - (l^2 + 2)v^2 \leq l^2v^2 - (l^2 + 2)v^2 = -2v^2,$$

which contradicts $q < 2v^2$.

Therefore, it is impossible that for $p = ((2n + 1)q)^2 + 2$ the equation $x^2 - py^2 = \pm q$ has a solution in integers.

§ 3. The class number of real subfields of a cyclotomic field

In this section, we shall consider the class number $h(p)$ of the real quadratic subfield $\mathbb{Q}(\sqrt{p})$ and the class number $H(4p)$ of the maximal real subfield $\mathbb{Q}(\zeta_{4p} + \zeta_{4p}^{-1})$ of the cyclotomic field $\mathbb{Q}(\zeta_{4p})$:

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{p}) \subset \mathbb{Q}(\zeta_{4p} + \zeta_{4p}^{-1}) \subset \mathbb{Q}(\zeta_{4p}).$$

From Theorems 1 and 2, we obtain first:

THEOREM 3. (1) *If $p = ((2n + 1)q)^2 - 2$ is a prime, where q is an odd prime satisfying $q \equiv 1$ or $3 \pmod{8}$ and $n \geq 0$ is an integer, then the class number $h(p)$ of the real quadratic field $\mathbb{Q}(\sqrt{p})$ is not equal to one except for the case of $p = 7$ ($n = 0, q = 3$).*

(2) *If $p = ((2n + 1)q)^2 + 2$ is a prime, where q is an odd prime satisfying $q \equiv 1$ or $7 \pmod{8}$ and $n \geq 0$ is an integer, then the class number $h(p)$ of the real quadratic field $\mathbb{Q}(\sqrt{p})$ is not equal to one i.e. $h(p) > 1$.*

Proof. (1) It is evident that a prime $p = ((2n + 1)q)^2 - 2$ with an integer $n \geq 0$ and an odd prime q satisfies $(p/q) = (-2/q)$, and so by the law of decomposition in quadratic fields, the prime q splits in $\mathbf{Q}(\sqrt{p})$ completely if and only if $(-2/q) = 1$ i.e. $q \equiv 1$ or $3 \pmod{8}$. Hence, moreover if $h(p) = 1$ is true, then by the Theorem 1 the equation $x^2 - py^2 = \pm q$ has at least one solution in integers x, y . This, however, contradicts the Theorem 2 except for the case of $p = 7$ ($n = 0, q = 3$). Therefore $h(p) = 1$ is impossible except for the case of $p = 7$ ($n = 0, q = 3$).

(2) Since a prime $p = ((2n + 1)q)^2 + 2$ with an integer $n \geq 0$ and an odd prime q satisfies $(p/q) = (2/q)$, by the law of decomposition in quadratic fields implies that the prime q splits in $\mathbf{Q}(\sqrt{p})$ completely if and only if $(2/q) = 1$ i.e. $q \equiv 1$ or $7 \pmod{8}$. Hence, moreover if $h(p) = 1$ is true, then by the Theorem 1 $x^2 - py^2 = \pm q$ has at least one solution in integers x, y . However, this contradicts the Theorem 2. Therefore $h(p) = 1$ is impossible, which proves the assertion of Theorem 3.

In order to prove Theorem 5, we need the following theorem⁴⁾:

THEOREM 4. *For a positive integer m , let ζ_m be a primitive m -th root of unity and denote by $H(m)$, $h(m)$ the class number of the field $K = \mathbf{Q}(\zeta_m + \zeta_m^{-1})$, $\mathbf{Q}(\sqrt{m})$ respectively. If a prime p satisfies $p \equiv 3 \pmod{4}$, then $h(p) \mid H(4p)$ holds.*

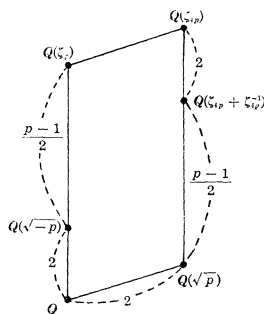
Proof. For a prime $p \equiv 3 \pmod{4}$, we first know that the real quadratic field $\mathbf{Q}(\sqrt{p})$ and the imaginary quadratic field $\mathbf{Q}(\sqrt{-p})$ are imbedded respectively in the real cyclotomic field $K = \mathbf{Q}(\zeta_{4p} + \zeta_{4p}^{-1})$ and the imaginary cyclotomic field $\mathbf{Q}(\zeta_p)$ by means of the Gauss sum

$$\sqrt{d} = \sum_{a \pmod{|d|}} \left(\frac{d}{a} \right) \zeta_{|d|}^a,$$

where d is the discriminant of a quadratic field $\mathbf{Q}(\sqrt{d})$ and (d/a) means the Kronecker symbol.

Next, we shall show $\mathbf{Q}(\zeta_p) \cap \mathbf{Q}(\sqrt{p}) = \mathbf{Q}$ and $\mathbf{Q}(\zeta_{4p}) = \mathbf{Q}(\sqrt{p}) \cdot \mathbf{Q}(\zeta_p)$. If we suppose $\mathbf{Q}(\zeta_p) \cap \mathbf{Q}(\sqrt{p}) \neq \mathbf{Q}$, namely $\mathbf{Q}(\sqrt{p}) \subset \mathbf{Q}(\zeta_p)$, then $\mathbf{Q}(\sqrt{p}) \subset \mathbf{Q}(\zeta_p + \zeta_p^{-1})$ follows. This, however, contradicts $p \equiv 3 \pmod{4}$, which shows $\mathbf{Q}(\zeta_p) \cap \mathbf{Q}(\sqrt{p}) = \mathbf{Q}$. Moreover, this assertion implies the following

4) This theorem was already stated by Yamaguchi in [4], with an incomplete proof, for any positive integer p satisfying $\varphi(p) > 4$. But, the theorem is not true in such a general form.



relation between degrees:

$$[Q(\sqrt{p}) \cdot Q(\zeta_p) : Q] = [Q(\sqrt{p}) : Q][Q(\zeta_p) : Q] = 2(p - 1).$$

On the other hand, since $[Q(\zeta_{4p}) : Q] = 2(p - 1)$ and $Q(\zeta_{4p}) \supset Q(\sqrt{p}) \cdot Q(\zeta_p)$, the assertion $Q(\zeta_{4p}) = Q(\sqrt{p}) \cdot Q(\zeta_p)$ is also true.

Furthermore, we can prove that no abelian unramified extension of $Q(\sqrt{p})$ is contained in $Q(\zeta_{4p} + \zeta_{4p}^{-1})$. For, if we suppose that there exists an abelian unramified extension field L of $Q(\sqrt{p})$ contained in $Q(\zeta_{4p} + \zeta_{4p}^{-1})$, then we have $n = [L : Q(\sqrt{p})] > 2$ because $[Q(\zeta_{4p} + \zeta_{4p}^{-1}) : Q(\sqrt{p})] = (p - 1)/2$ is odd. Hence, the ramification index $e(p)$ of p in $Q(\zeta_{4p})/Q$, which is a divisor of $2(p - 1)/n$, is less than $p - 1$ i.e. $e(p) < p - 1$. However, since p is completely ramified in $Q(\zeta_p)/Q$, $e(p)$ is not less than $p - 1$ i.e. $e(p) \geq p - 1$. This is a contradiction, which proves our assertion.

Finally, from this assertion, it follows immediately by Hasse-Chevalley's theorem⁵⁾ that the assertion of Theorem 4 $h(p) | H(4p)$ is true.

THEOREM 5. (1) *If $p = ((2n + 1)q)^2 - 2$ is a prime, where q is an odd prime satisfying $q \equiv 1$ or $3 \pmod{8}$ and $n \geq 0$ is an integer, then the class number $H(4p)$ of $Q(\zeta_{4p} + \zeta_{4p}^{-1})$ is greater than one except for the case of $p = 7$ ($n = 0, q = 3$).*

(2) *If $p = ((2n + 1)q)^2 + 2$ is a prime, where q is an odd prime satisfying $q \equiv 1$ or $7 \pmod{8}$ and $n \geq 0$ is an integer, then the class number $H(4p)$ of $Q(\zeta_{4p} + \zeta_{4p}^{-1})$ is greater than one: $H(4p) > 1$.*

Proof. Since $p = ((2n + 1)q)^2 \pm 2 \equiv 3 \pmod{4}$, the assertion of the Theorem $H(4p) > 1$ follows immediately from Theorem 3 and 4.

Finally, we give the values of all primes p less than 10^5 satisfying

5) Cf. [2].

the conditions in Theorem 3 and the class number $h(p)$ of the corresponding real quadratic fields $\mathbf{Q}(\sqrt{p})^6$.

$$p = ((2n + 1)q)^2 - 2$$

p	n	q	$h(p)$	p	n	q	$h(p)$
7#	0	3	1#	357	0	19	3
79	1	3	3	1,087*	1	11	7
223	2	3	3	1,847	0	43	3
439	3	3	5	3,023	2	11	3
727	4	3	5	5,927	3	11	5
1,087	5	3	7	7,919	0	89	7
3,967	10	3	5	11,447	0	107	7
4,759	11	3	13	14,159	3	17	9
5,623	12	3	9	14,639	5	11	17
8,647	15	3	13	17,159	0	131	15
13,687	19	3	21	19,319	0	139	11
18,223	22	3	17	31,327*	1	59	27
31,327	29	3	27	42,023	2	41	15
33,487	30	3	19	44,519	0	211	11
53,359	38	3	37	53,359*	10	11	37
56,167	39	3	27	54,287	0	233	15
71,287	44	3	19	61,007	6	19	15
74,527	45	3	23	64,007	11	11	11
77,839	46	3	37	66,047	0	257	13
81,223	47	3	33	71,287*	1	89	19
91,807	50	3	45	81,223*	7	19	33
95,479	51	3	33	90,599	3	43	19
99,223	52	3	29	97,967	0	313	25

$$p = ((2n + 1)q)^2 + 2$$

p	n	q	$h(p)$	p	n	q	$h(p)$
443	1	7	3	56,171	1	79	11
11,027	7	7	9	65,027	7	17	21
15,131	1	41	15	74,531	19	7	17
21,611	10	7	15	95,483	1	103	11
47,963	1	73	9				

indicates only one exceptional case with class number $h(p) = 1$.

* indicates that the prime has appeared in the case of $q = 3$

6) For this purpose we referred to Wada's table of class numbers of real quadratic fields in [7].

REFERENCES

- [1] G. Degert, Über die Bestimmung der Grundeinheit gewisser reell-quadratischer Zahlkörper, Abh. Math. Sem. Univ. Hamburg, **22** (1958), 92–97.
- [2] N. C. Ankeny, S. Chowla and H. Hasse, On the class-number of the maximal real subfield of a cyclotomic field, J. reine angew. Math., **217** (1965), 217–220.
- [3] H. Hasse, Über mehrklassige, aber eingeschlechtige reell-quadratische Zahlkörper, Elemente der Mathematik, **20** (1965), 49–72.
- [4] I. Yamaguchi, On the class-number of the maximal real subfield of a cyclotomic field, J. reine angew. Math., **272** (1975), 217–220.
- [5] S.-D. Lang, Note on the class-number of the maximal real subfield of a cyclotomic field, J. reine angew. Math., **290** (1977), 70–72.
- [6] H. Takeuchi, On the class-number of the maximal real subfield of a cyclotomic field, Canadian J. Math., **33** (1981), 55–58.
- [7] H. Wada, A table of ideal class numbers of real quadratic fields, Kökyūroku in Math., No. **10** (1981), Sophia Univ., Tokyo.

*Department of Mathematics
College of General Education
Nagoya University
Chikusa-ku, Nagoya 464
Japan*

