Imaginary quadratic fields satisfying
the Hilbert–Speiser type condition for a small prime $p$

by

HUMIO ICHIMURA (Ibaraki)
and HIROKI SUMIDA-TAKAHASHI (Tokushima)

1. Introduction. Let $p$ be a prime number, and $\Gamma = \Gamma_p$ the cyclic group of order $p$; $\Gamma = \mathbb{F}_p^+$, where $\mathbb{F}_p^+$ is the additive group of the finite field $\mathbb{F}_p$ of $p$ elements. We say that a number field $F$ satisfies condition $(A_p)$ if for any tame $\Gamma$-extension $N/F$, $\mathcal{O}_N$ is cyclic over the group ring $\mathcal{O}_F\Gamma$. Here, $\mathcal{O}_F$ is the ring of integers of $F$. It is well known by work of Hilbert and Speiser that the rationals $\mathbb{Q}$ satisfy $(A_p)$ for all primes $p$. In [6, Theorem 1], Greither et al. gave a necessary condition for a number field $F$ to satisfy $(A_p)$ in terms of (a subgroup of) the ray class group of $F$ defined modulo $p$, using a theorem of McCulloh [20, 21]. Applying that condition, they proved that $F \neq \mathbb{Q}$ does not satisfy $(A_p)$ for infinitely many primes $p$ ([6, Theorem 2]). Thus, it is of interest to determine which number fields $F$ satisfy $(A_p)$. Several authors [3, 4, 11–13] obtained some results on the problem using the above mentioned condition (and some other results such as a theorem of Gómez Ayala [5, Theorem 2.1]). For instance, it was shown by Carter [3, Corollary 3] that an imaginary quadratic field $F = \mathbb{Q}(\sqrt{-d})$ with $d > 0$ square free satisfies $(A_2)$ if and only if $d = 1, 3$ or 7. Further, all quadratic fields satisfying $(A_3)$ were determined independently in [3, Corollary 5] and [12, Proposition]. There are exactly four imaginary and eight real ones satisfying $(A_3)$. The purpose of this paper is to determine all imaginary quadratic fields satisfying $(A_p)$ for $p = 5, 7$ or 11. The result is as follows:

**Theorem 1.** An imaginary quadratic field $F = \mathbb{Q}(\sqrt{-d})$ with a square free positive integer $d$ satisfies the condition $(A_5)$ if and only if $d = 1$ or 3. It satisfies $(A_7)$ if and only if $d = 3$. No imaginary quadratic field satisfies $(A_{11})$.

As in [6], the above mentioned theorem of McCulloh plays an important role in proving Theorem 1. In Section 2, we recall McCulloh’s theorem and

2000 Mathematics Subject Classification: 11R33, 11R11.
several of its consequences including the above mentioned condition for \((A_p)\) in [6]. In Section 3, we give some conditions for an imaginary quadratic field to satisfy \((A_p)\) and prove Theorem 1. In Section 4, we review some topics on subfields of the \(p\)-cyclotomic field \(\mathbb{Q}(\zeta_p)\) satisfying \((A_p)\).

2. Consequences of McCulloh’s theorem. In this section, we recall a theorem of McCulloh [20, 21] and several of its consequences. Let \(F\) be a number field. For an integer \(a \in \mathcal{O}_F\), let \(Cl_F(a)\) be the ray class group of \(F\) defined modulo the ideal \(a\mathcal{O}_F\). We simply write \(Cl_F = Cl_F(1)\), the absolute class group of \(F\). Let \(Cl(O_F^+\Gamma)\) be the locally free class group of the group ring \(O_F^+\Gamma\), and let \(Cl^0(O_F^+\Gamma)\) be the kernel of the homomorphism \(Cl(O_F^+\Gamma) \to Cl_F\) induced from the augmentation \(O_F^+\Gamma \to O_F\). The class group \(Cl^0(O_F^+\Gamma)\) is known to be a quotient of some copies of the ray class group \(Cl(\zeta_p)(p)\), but it is a quite complicated object in general. Let \(R(O_F^+\Gamma)\) be the subset of \(Cl(O_F^+\Gamma)\) consisting of the locally free classes \([\mathcal{O}_N]\) for all tame \(\Gamma\)-extensions \(N/F\). It follows that \(F\) satisfies \((A_p)\) if and only if \(R(O_F^+\Gamma) = \{0\}\). It is known that \(R(O_F^+\Gamma) \subseteq Cl^0(O_F^+\Gamma)\). Let \(G = \mathbb{F}_p^\times\) be the multiplicative group of \(\mathbb{F}_p\). Through the natural action of \(G\) on \(\Gamma = \mathbb{F}_p^\times\), the group ring \(\mathbb{Z}G\) acts on \(Cl(O_F^+\Gamma)\). Let \(S_G\) be the classical Stickelberger ideal of the group ring \(\mathbb{Z}G\). For the definition, see Washington [26, Chapter 6].

**Theorem 2 ([21]).** Under the above setting, we have

\[
R(O_F^+\Gamma) = Cl^0(O_F^+\Gamma) S_G.
\]

Let \(\mathcal{O}_F^\times\) be the group of units of a number field \(F\). For an integer \(a \in \mathcal{O}_F\), let \([\mathcal{O}_F^\times]/a\) be the subgroup of the multiplicative group \((\mathcal{O}_F/a)^\times\) consisting of the classes containing a unit of \(F\). The quotient \((\mathcal{O}_F/a)^\times/([\mathcal{O}_F^\times]/a)\) is a subgroup of the ray class group \(Cl_F(a)\). Greither et al. [6] proved the following relation between condition \((A_p)\) and \(Cl_F(p)\) from Theorem 2 by studying a canonical subgroup of \(Cl(O_F^+\Gamma)\), called the Swan subgroup.

**Proposition 1 ([6, Theorem 1]).** Assume that a number field \(F\) satisfies condition \((A_p)\). Then the exponent of the quotient \((\mathcal{O}_F/p)^\times/([\mathcal{O}_F^\times]/p)\) divides \((p - 1)/2\) when \(p \geq 3\), and \((\mathcal{O}_F/p)^\times = [\mathcal{O}_F^\times]/p\) when \(p = 2\).

The following is obtained from Proposition 1 and [5, Theorem 2.1].

**Proposition 2 ([11, Proposition 2]).** A number field \(F\) satisfies condition \((A_2)\) if and only if the ray class group \(Cl_F(2)\) is trivial.

Similar conditions for \((A_2)\) are also given in [3, Theorem 2] and in Herrng [9, Theorem 2.1]. In view of Proposition 2, we let \(p \geq 3\) in the following. To give another consequence of Theorem 2, we need to recall a “Stickelberger ideal” associated to a subgroup of \(G\). Let \(H\) be a subgroup of \(G\). For an el-
Quadratic fields satisfying the Hilbert–Speiser type condition

Given an element $\alpha \in \mathbb{Z}G$, let

$$\alpha_H = \sum_{\sigma \in H} a_{\sigma} \sigma \in \mathbb{Z}H \quad \text{with} \quad \alpha = \sum_{\sigma \in G} a_{\sigma} \sigma.$$ 

In other words, $\alpha_H$ is the $H$-part of $\alpha$. In [14], we defined the Stickelberger ideal $S_H$ of $\mathbb{Z}H$ by

$$S_H = \{ \alpha_H \mid \alpha \in S_G \} \subseteq \mathbb{Z}H.$$ 

Several properties of the ideal $S_H$ are studied in [14, 15, 17, 18]. For an integer $i \in \mathbb{Z}$, let $\overline{i}$ be the class in $\mathbb{F}_p = \mathbb{Z}/p$ containing $i$. It is known that the ideal $S_H$ is generated over $\mathbb{Z}$ by the Stickelberger elements

$$\theta_{H,r} = \sum_{i} \left\lfloor \frac{r \overline{i}}{p} \right\rfloor \cdot \overline{i}^{-1} \in \mathbb{Z}H \quad \text{(1)}$$

for all integers $r \in \mathbb{Z}$. Here, $i$ runs over the integers with $1 \leq i \leq p-1$ and $\overline{i} \in H$, and for a real number $x$, $\lfloor x \rfloor$ is the largest integer $\leq x$. Let $N_H$ be the norm element of $\mathbb{Z}H$. It follows that

$$N_H = -\theta_{H,-1} \in S_H.$$ 

Letting $\varrho$ be a generator of $H$, put

$$n_H = \begin{cases} 1 + \varrho + \cdots + \varrho^{|H|/2-1} & \text{if } |H| \text{ is even}, \\ 1 & \text{if } |H| \text{ is odd}. \end{cases}$$

As is easily seen, the ideal $\langle n_H \rangle = n_H \mathbb{Z}H$ does not depend on the choice of $\varrho$. It is known that $S_H \subseteq \langle n_H \rangle$ ([18, Lemma 1]) and that the quotient $\langle n_H \rangle / S_H$ is a finite abelian group whose order divides the relative class number $h_p^-$ of the $p$-cyclotomic field $\mathbb{Q}(\zeta_p)$ ([18, Theorem 2]):

$$[\langle n_H \rangle : S_H] \mid h_p^- \quad \text{(2)}$$

Let $F$ be a number field, and $K = F(\zeta_p)$. We naturally identify the Galois group $\text{Gal}(K/F)$ with a subgroup $H$ of $G$ through the Galois action on $\zeta_p$. Then the group ring $\mathbb{Z}H$ acts on several objects associated to $K/F$. Let $\pi = \zeta_p - 1$. The following assertion was obtained from Theorem 2 and Proposition 1.

**Proposition 3** ([13, Theorem 5]). Let $F$ be a number field, and let $K = F(\zeta_p)$ and $H = \text{Gal}(K/F) \subseteq G$. If $F$ satisfies $(A_p)$, then

$$\text{Cl}_K(\pi)^{S_H} = \{0\} \quad \text{and} \quad \text{Cl}_K(p)^{S_H} \cap \text{Cl}_K(p)^H = \{0\}.$$ 

Here, $\text{Cl}_K(p)^H$ is the Galois invariant part.

It is known that the converse of this assertion holds when $p = 3$ ([12, Theorem 2]). The following is a consequence of Proposition 3.

**Proposition 4.** Let $F$ and $K$ be as in Proposition 3. Assume that $F$ satisfies $(A_p)$ and that the norm map $\text{Cl}_K \to \text{Cl}_F$ is surjective. Then...
the natural map $\text{Cl}_F \to \text{Cl}_K$ is trivial. In particular, the exponent of $\text{Cl}_F$ divides $[K : F]$.

Proof. By the assumption, any ideal class $c \in \text{Cl}_F$ is of the form $c = d^N_H$ for some $d \in \text{Cl}_K$. However, when $F$ satisfies $(A_p)$, the class $d^N_H$ is trivial in $\text{Cl}_K$ by Proposition 3 and $N_H \in S_H$. $
abla$

When $F/\mathbb{Q}$ is unramified at $p$, the Galois group $\text{Gal}(K/F)$ is naturally identified with $G = \mathbb{F}_p^\times$ through the Galois action on $\zeta_p$. The following is a consequence of Theorem 2.

**Proposition 5.** Assume that $F/\mathbb{Q}$ is unramified at $p$, and let $K = F(\zeta_p)$. Then $F$ satisfies condition $(A_p)$ if and only if the Stickelberger ideal $S_G$ annihilates the ray class group $\text{Cl}_K(\pi)$.

**Proof.** Brinkhuis [2, Proposition (2.2)] proved that the $\mathbb{Z}G$-module $\text{Cl}_0(\mathcal{O}_F\Gamma)$ is naturally isomorphic to the ray class group $\text{Cl}_K(\pi)$ when $F/\mathbb{Q}$ is unramified at $p$. Hence, the assertion follows immediately from Theorem 2. $
abla$

Though the following assertion is irrelevant to the proof of Theorem 1, it might be of some interest to the reader. For a CM-field $K$, let $\text{Cl}_K^-$ be the kernel of the norm map $\text{Cl}_K \to \text{Cl}_K^+$ where $K^+$ is the maximal real subfield of $K$.

**Proposition 6.** Let $F$ be a totally real number field, and $K = F(\zeta_p)$. If $F$ satisfies $(A_p)$, then the exponent of $\text{Cl}_K^-$ divides $2h_p^−$.

**Proof.** Let $H = \text{Gal}(K/F) \subseteq G$, and let $\varphi$ be a generator of $H$. As $F$ is totally real, $|H|$ is even and $J = \varphi^{\frac{|H|}{2}}$ is the complex conjugation in $H$. We easily see that $(1 - \varphi)n_H = 1 - J$, and that $n_H h_p^− \in S_H$ by (2). Hence, $(1 - J)h_p^− \in S_H$. Assume that $F$ satisfies $(A_p)$. Then, by Proposition 3, $(1 - J)h_p^−$ annihilates $\text{Cl}_K$. The assertion follows from this. $
abla$

**3. Imaginary quadratic fields.** In this section, let $p \geq 3$ be an odd prime number, and $F = \mathbb{Q}(\sqrt{-d})$ an imaginary quadratic field with a square free positive integer $d$.

**Lemma 1.** When $p$ is ramified in $F/\mathbb{Q}$, $F$ satisfies $(A_p)$ if and only if $p = 3$ and $F = \mathbb{Q}(\sqrt{-3})$.

**Proof.** The “only if” part is an easy consequence of Proposition 1 since $(\mathcal{O}_F/p)^\times$ is cyclic of order $p(p - 1)$ when $p$ ramifies in $F$. The “if” part is due to [5, p. 110]. $
abla$

**Lemma 2.**

(I) Let $p = 3$ or 5. If $F \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$ and $p$ is inert in $F$, then $F$ does not satisfy $(A_p)$.
(II) Let \( p \geq 7 \). If \( p \) is inert in \( F \), then \( F \) does not satisfy \((A_p)\).

**Proof.** This is an easy consequence of Proposition 1 since \((\mathcal{O}_F/p)^{\times}\) is cyclic of order \( p^2 - 1 \) when \( p \) is inert in \( F \). \( \blacksquare \)

In all what follows, we exclude the case where \( p = 3 \) and \( F = \mathbb{Q}(\sqrt{-3}) \), and we let \( K = F(\zeta_p) \). Hence, by Lemma 1, if \( F \) satisfies \((A_p)\), then \( F/\mathbb{Q} \) is unramified at \( p \) and the Galois group \( \text{Gal}(K/F) \) is naturally identified with \( G = \mathbb{F}_p^{\times} \).

**Lemma 3.** If \( F \) satisfies \((A_p)\), then the exponent of the class group \( \text{Cl}_F \) divides 2.

**Proof.** We use a standard argument in [26, pp. 289–290]. Assume that \( F \) satisfies \((A_p)\). As \( F/\mathbb{Q} \) is unramified at \( p \), \( K/F \) is totally ramified at the primes over \( p \). Hence, the natural map \( \text{Cl}_F \to \text{Cl}_K \) is trivial by Proposition 4. Let \( A \) be an arbitrary ideal of \( F \) relatively prime to \( p \). We have \( A\mathcal{O}_K = \alpha\mathcal{O}_K \) for some \( \alpha \in K^{\times} \). Let \( \theta \) be a generator of \( G \), and \( J \) a generator of \( \text{Gal}(F/\mathbb{Q}) = \text{Gal}(K/K^+) \) where \( K^+ \) is the maximal real subfield of \( K \). As \( A \) is an ideal of \( F \), we have \( \alpha^{1-e} = \varepsilon \in \mathcal{O}_K^{\times} \). On the other hand, \( A 1+J = \beta\mathcal{O}_F \) for some \( \beta \in \mathcal{O}_K^{\times} \). Hence, \( \alpha^{1+J} = \beta\theta \) for some unit \( \eta \in \mathcal{O}_K^{\times} \). It follows that

\[
\varepsilon^{1+J} = (\alpha^{1+J})^{1-e} = \eta^{1-e}
\]

as \( \beta \in \mathcal{O}_K^{\times} \). Putting \( \alpha_1 = \alpha^2/\eta \), we have

\[
(3) \quad \alpha_1\mathcal{O}_K = A^2\mathcal{O}_K.
\]

Let

\[
(4) \quad \varepsilon_1 = \alpha_1^{e-1} = \varepsilon^{-2}\eta^{1-e} \in \mathcal{O}_K^{\times}.
\]

Then

\[
\varepsilon_1^{1+J} = \varepsilon^{-2(1+J)}\theta^{1-e}(1+J) = \theta^{(1-J)(e-1)}.
\]

Hence, \( \varepsilon_1 \) is a root of unity in \( K \) by a theorem on units of a CM-field (cf. [26, Theorem 4.12]). Let \( \mu_p \) be the group of \( p \)th roots of unity in \( K \). We consider separately the cases when \( \varepsilon_1 \in \mu_p \) or not.

**The case** \( \varepsilon_1 \notin \mu_p \). Since the map \( \varrho - 1 : \mu_p \to \mu_p \) is an isomorphism, we can write \( \varepsilon_1 = \zeta^{e-1} \) for some \( \zeta \in \mu_p \). Hence, it follows from (4) that \( (\alpha_1/\zeta)^{\varrho} = \alpha_1/\zeta \) and \( \alpha_1/\zeta \in F^{\times} \). Therefore, by (3), \( A^2 \) is a principal ideal of \( F \).

**The case** \( \varepsilon_1 \notin \mu_p \). As the class groups of \( \mathbb{Q}(\sqrt{-1}) \) and \( \mathbb{Q}(\sqrt{-3}) \) are trivial, we may well assume that \( F \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3}) \). Then the condition \( \varepsilon_1 \notin \mu_p \) implies that \( -\varepsilon_1 \notin \mu_p \), and hence, \( -\varepsilon_1 = \zeta^{e-1} \) for some \( \zeta \in \mu_p \). On the other hand, we have \( -1 = (\sqrt{p^\ast})^{e-1} \) where \( p^\ast = p \) if \( p \equiv 1 \mod 4 \) and \( p^\ast = -p \) otherwise. Therefore, \( \varepsilon_1 = (\sqrt{p^\ast}\zeta)^{e-1} \). Hence, it follows from (4)
that
\[(\alpha_1/\sqrt{p^r}\zeta)^q = \alpha_1/\sqrt{p^r}\zeta \quad \text{and} \quad \alpha_1/\sqrt{p^r}\zeta \in F^\times.\]
This implies that \(p\) is ramified in \(F\) as \(\mathfrak{a}\) is relatively prime to \(p\). This is a contradiction. ■

Lemma 3 asserts that if the exponent of \(\text{Cl}_F\) is greater than 2, then \(F\) does not satisfy \((A_p)\) for any prime \(p\). All imaginary quadratic fields \(F\) with \(\text{Cl}_F^2 = \{0\}\) were determined by Weinberger [27, Theorem 1] with possibly one exception. A table of such \(F\)’s is given in Miyada [22, p. 539]. There are exactly 65 (or possibly 66) such \(F\). In particular, we obtain the following:

**Proposition 7.** For each prime number \(p\), there exist at most 65 (or possibly 66) imaginary quadratic fields satisfying condition \((A_p)\).

**Lemma 4.** Let \(p = 5\), and \(E = F(\sqrt{5})\). If \(F\) satisfies \((A_5)\), then the natural map \(\text{Cl}_F \to \text{Cl}_E\) is trivial.

**Proof.** Assume that \(F\) satisfies \((A_5)\). Let \(\varphi\) be a generator of \(G = \text{Gal}(K/F)\). We have \(S_G = \langle 1 + \varphi \rangle\) by \(h_5 = 1\) and (2). By the assumption and Proposition 3 or 5, \(c^{1+q} = 1\) for any \(c \in \text{Cl}_K\). As the norm map \(\text{Cl}_K \to \text{Cl}_F\) is surjective, this relation holds for any \(c \in \text{Cl}_E\). As the norm map \(\text{Cl}_E \to \text{Cl}_F\) is surjective, any class \(d \in \text{Cl}_F\) is of the form \(d = N_{E/F}(c) = c^{1+q}\) for some \(c \in \text{Cl}_E\). Therefore, we obtain the assertion. ■

**Lemma 5.** Let \(p\) be a prime number with \(p \equiv 3 \mod 4\), and \(E = F(\sqrt{-p})\). If \(F\) satisfies \((A_p)\), then the natural map \(\text{Cl}_F \to \text{Cl}_E\) is trivial.

**Proof.** Assume that \(F\) satisfies \((A_p)\). Let \(\mathfrak{a}\) be an ideal of \(F\). By Proposition 4, \(\mathfrak{a}\mathcal{O}_K = \alpha\mathcal{O}_K\) for some \(\alpha \in K^\times\). Hence, \(\mathfrak{a}[K:E]\mathcal{O}_E = \beta\mathcal{O}_E\) with \(\beta = N_{K/E}(\alpha)\). This implies that \(\mathfrak{a}\mathcal{O}_E\) is a principal ideal since \([K:E]\) is odd by the assumption on \(p\), and \(\mathfrak{a}^2\) is principal in \(F\) by Lemma 3. ■

**Lemma 6.** Let \(p\) be a prime number with \(p \equiv 3 \mod 4\) or \(p = 5\). If \(F\) satisfies \((A_p)\), then \(\text{Cl}_F\) is isomorphic to the abelian group \((\mathbb{Z}/2)^{\oplus R}\) with \(R \leq 2\).

**Proof.** Let \(H_F^{(2)}/F\) be the maximal unramified abelian extension of exponent 2, and let \(E\) be as in Lemmas 4 and 5. Assume that \(F\) satisfies \((A_p)\). Then \([H_F^{(2)} : F] = [H_F^{(2)} E : E]\) since \(E/F\) is totally ramified at the primes over \(p\). Let \(t\) be the number of prime numbers which ramify in \(F\). Let \(\lambda_1, \ldots, \lambda_r\) (resp. \(\mu_1, \ldots, \mu_s\)) be all the odd prime numbers which ramify in \(F\) and are congruent to 1 (resp. 3) modulo 4. The 2-rank of \(\text{Cl}_F\) equals \(t - 1\) by a well known theorem on quadratic fields (cf. Hecke [8, Theorem 132]). Hence, by Lemma 3, it suffices to show that \(t \leq 3\) since we are assuming that \(F\) satisfies \((A_p)\). It is well known and easy to show that
\[H_F^{(2)} = F(\sqrt{\lambda_i}, \sqrt{-\mu_j} | 1 \leq i \leq r, 1 \leq j \leq s).\]
Let $\ell$ be any one of the prime numbers $\lambda_i$ and $\mu_j$, and let $\mathfrak{l}$ be the prime ideal of $F$ over $\ell$. By Lemmas 4 and 5, the ideal $\mathfrak{l}\mathcal{O}_E$ is principal. This implies that $\ell = \varepsilon x^2$ for some unit $\varepsilon \in \mathcal{O}_E^\times$ and $x \in E^\times$. Therefore,

$$H^{(2)}_{F^2} E \subseteq E(\sqrt{\varepsilon} \mid \varepsilon \in \mathcal{O}_E^\times).$$

Now, from the above, it follows that

$$2t - 1 = [H^{(2)}_{F^2} : F] = [H^{(2)}_{F^2} E : E] = 1, 2 \text{ or } 4$$

since the group $\mathcal{O}_E^\times$ is generated by two elements. Therefore, $t \leq 3$. 

For a number field $N$ and a prime number $q$, let $Cl_N[q]$ be the Sylow $q$-subgroup of the class group $Cl_N$.

**Lemma 7.** Let $p \geq 7$ be a prime number with $p \equiv 3 \pmod{4}$. Let $K = F(\zeta_p)$, and let $N$ be an intermediate field of $K/F$ with $2 \nmid [K : N]$. If the 2-part $Cl_N[2]$ is nontrivial and cyclic as an abelian group, then $F$ does not satisfy $(A_p)$.

**Proof.** Assume that $Cl_N[2]$ is nontrivial and cyclic, but $F$ satisfies $(A_p)$. Let $c$ be a generator of the cyclic group $Cl_N[2]$. Then

$$(5) \quad c^\sigma \equiv c \pmod{2Cl_N[2]}$$

for all $\sigma \in G$. As $[K : N]$ is odd, the natural map $Cl_N[2] \rightarrow Cl_K$ is injective. Let $\overline{c}$ and $\overline{Cl}_N[2]$ be the images of $c$ and $Cl_N[2]$ under this injection. As $F$ satisfies $(A_p)$, the Stickelberger element $\theta_{G,2}$ kills $\overline{c}$. We easily see that the augmentation $ZG \rightarrow Z$ maps the element $\theta_{G,2}$ to $(p - 1)/2$ from the definition (1). Therefore, it follows from (5) that

$$1 = \overline{c}\theta_{G,2} \equiv \overline{c}^{(p-1)/2} \pmod{2\overline{Cl}_N[2]}.$$

This implies that $c^{(p-1)/2} \in 2Cl_N[2]$ as $Cl_N[2] \rightarrow Cl_K$ is injective. Hence, $c \in 2Cl_N[2]$ as $(p - 1)/2$ is odd. This is a contradiction. 

For a number field $N$, let $h_N$ be the class number of $N$.

**Lemma 8.** Let $p$ be a prime number with $p \equiv 3 \pmod{4}$ and $p \leq 19$, and let $E = F(\sqrt{-p})$. If the class number $h_E$ is divisible by an odd prime number $q$ relatively prime to $(p - 1)/2$, then $F$ does not satisfy $(A_p)$.

**Proof.** As $q$ is relatively prime to $(p - 1)/2$, the natural map $Cl_E[q] \rightarrow Cl_K$ is injective. Let $c$ be a class in $Cl_E$ of order $q$, and $\overline{c}$ its lift to $K$. The class $\overline{c}$ is nontrivial. Let $g$ be a generator of $G = Gal(K/F)$. Assume that $F$ satisfies $(A_p)$. Then $c^g = c^{-1}$ since $h_F$ is a power of 2 by Lemma 3. Hence,

$$(6) \quad \overline{c}^g = \overline{c}^{-1}.$$
The condition $p \leq 19$ is equivalent to $h_p^{-1} = 1$ (cf. [26, Corollary 11.18]). Hence, by (2), the Stickelberger ideal $S_G$ is generated by $n_G$. Since $F$ satisfies $(A_p)$, we see that $n_G$ annihilates $Cl_K$ by Proposition 3 or 5. As $(p-1)/2$ is odd, we see from (6) that
\[
1 = \zeta^{n_G} = \zeta^{(1+1)+\cdots+(1+1)+1} = \zeta.\]
This is a contradiction. ■

**Lemma 9.** Let $F$ be a quadratic field not necessarily imaginary, and let $p$ be a prime number splitting in $F$. Let $\mathfrak{P}_1$ and $\mathfrak{P}_2$ be the prime ideals of $K = F(\zeta_p)$ over $p$. Then the Stickelberger ideal $S_G$ annihilates $(O_K/\pi)^{\times}/[O_K^{\times}]$ if and only if there exists a unit $\varepsilon \in O_K^{\times}$ satisfying
\[
\varepsilon \equiv 1 \text{ mod } \mathfrak{P}_1 \quad \text{and} \quad \varepsilon \equiv -1 \text{ mod } \mathfrak{P}_2.\]

**Proof.** For brevity, put $X = (O_K/\pi)^{\times}/[O_K^{\times}]$. We have
\[
(O_K/\pi)^{\times} = (O_K/\mathfrak{P}_1)^{\times} \oplus (O_K/\mathfrak{P}_2)^{\times} = F_p^{\times} \oplus F_p^{\times}.\]
The Galois group $G = \text{Gal}(K/F)$ fixes the prime ideal $\mathfrak{P}_1$, and it acts trivially on $(O_K/\mathfrak{P}_1)^{\times}$. The augmentation $\iota_G : ZG \to Z$ maps both $n_G$ and $\theta_{G,2}$ to $(p-1)/2$. Hence, we see from (2) that $\iota_G$ maps the ideal $S_G \subseteq ZG$ onto the ideal of $Z$ generated by $(p-1)/2$. Therefore, the condition $X^{S_G} = \{0\}$ is equivalent to
\[
(O_K/\pi)^{\times}((p-1)/2) \subseteq [O_K^{\times}]_\pi.\]
From this, we obtain the assertion. ■

**Lemma 10.** Let $F = \mathbb{Q}(\sqrt{-d})$ be an imaginary quadratic field with a square free positive integer $d$, and let $p$ be a prime number splitting in $F$. There exists a unit $\varepsilon \in O_K^{\times}$ satisfying (7) in the following two cases:

(I) $d = 1$,

(II) $d$ is a prime number with $d \neq 1$ mod 4, and $p \equiv 3$ mod 4.

**Proof.** We first show the assertion in case (II). Let $E = F(\sqrt{-p})$. It is well known that the unit index $Q_E$ of the imaginary abelian field $E$ equals 2 by Hasse [7, p. 76]. We apply the classical argument used to show $Q_E = 2$. Let $E^+ = \mathbb{Q}(\sqrt{pd})$ be the maximal real subfield of $E$. Let $Q_d$ be the prime ideal of $E^+$ over the prime $d$; $(d) = Q_d^2$. From the conditions on $d$ and $p$, we see that the class number of $E^+$ is odd by genus theory. Hence, there exist $u, v \in \mathbb{Z}$ such that $u^2 - v^2pd = \pm 4d$. It follows that $u = u'd$ for some $u' \in \mathbb{Z}$ and $\eta = (u'\sqrt{-d} + v\sqrt{-p})/2$ is a unit of $O_E$. Let $\mathfrak{P}_1$ and $\mathfrak{P}_2$ be the prime ideals of $K$ over $p$. Let $a \in \mathbb{Z}$ be an integer such that $\sqrt{-d} \equiv a$ mod $\mathfrak{P}_1$. We see that $\sqrt{-d} \equiv -a$ mod $\mathfrak{P}_2$. If $\eta \equiv b$ mod $\mathfrak{P}_1$ and $\eta \equiv -b$ mod $\mathfrak{P}_2$ for some integer $b$ with $1 \leq b \leq p-1$. Let $\delta_b = 1 + \zeta_p + \cdots + \zeta_p^{b-1}$ be a cyclotomic unit in $K$. Then, since $\delta_b \equiv b$ mod $\pi$, the unit $\varepsilon = \eta/\delta_b$ satisfies (7).
In case (I), we can similarly show the assertion by taking $\varepsilon = \sqrt{-1}$ times a suitable cyclotomic unit of $K$. 

**Proof of Theorem 1.** By Lemma 6, we do not need the conditional result of Weinberger [27] mentioned before. The imaginary quadratic fields $F$ with $h_F = 1$ were determined by Stark [24]. Those with $h_F = 2$ were determined independently by Stark [25] and Montgomery and Weinberger [23], and those with $h_F = 4$ by Arno [1]. By genus theory, we can easily pick out those with $Cl_F = (\mathbb{Z}/2)^{\oplus 2}$ from Arno’s result. Using these results and Lemmas 1 and 2, we obtain the following lists.

**Lemma 11.** An imaginary quadratic field $F = \mathbb{Q}(\sqrt{-d})$ may satisfy $(A_5)$ only when $d$ is one of the following:

(i) $1, 3, 11, 19$; (ii) $6, 51, 91$; (iii) $21$.

**Lemma 12.** An imaginary quadratic field $F = \mathbb{Q}(\sqrt{-d})$ may satisfy $(A_7)$ only when $d$ is one of the following:

(i) $3, 19$; (ii) $5, 6, 10, 13, 115, 187$; (iii) $33, 195$.

**Lemma 13.** An imaginary quadratic field $F = \mathbb{Q}(\sqrt{-d})$ may satisfy $(A_{11})$ only when $d$ is one of the following:

(i) $2, 7, 19, 43$; (ii) $6, 10, 13, 35, 51, 123, 403$; (iii) $21, 30, 57, 85, 195, 435, 483$.

In the above lists, those $F$ or $d$ in the first groups satisfy $h_F = 1$, those in the second groups have $h_F = 2$, and those in the last groups, $Cl_F = (\mathbb{Z}/2)^{\oplus 2}$. In the following, let $K = F(\zeta_p)$ and $E$ be the intermediate field of $K/F$ with $[E : F] = 2$. Let $\varrho$ be a generator of $G = \text{Gal}(K/F)$. By (2), $S_G$ is generated by

$$n_G = 1 + \varrho + \cdots + \varrho^{(p-1)/2-1}.$$ 

All the following calculations were done using KASH.

**The case** $p = 5$. We checked that the natural map $Cl_F \to Cl_E$ is not trivial when $d = 6, 51, 91$ or $21$. Hence, by Lemma 4, $F$ does not satisfy $(A_5)$ for these $d$. When $d = 1$ or $3$, we have $Cl_K = \{0\}$. When $d = 1$, we see that $Cl_K(\pi)^{S_G} = \{0\}$ by Lemmas 9 and 10. When $d = 3$, we checked $Cl_K(\pi)^{S_G} = \{0\}$ by explicitly finding a system of fundamental units of $K$. Hence, by Proposition 5, $F$ satisfies $(A_5)$ for $d = 1$ or $3$. When $d = 11$ (resp. $19$), we see that $Cl_K = \mathbb{Z}/2$ (resp. $\mathbb{Z}/4$) and $Cl_K^{S_G} = \{0\}$. We chose an ideal $\mathfrak{A}$ of $K$ such that the class $[\mathfrak{A}]$ generates the cyclic group $Cl_K$. We checked that a generator $\alpha$ of the principal ideal $\mathfrak{A}^{1+\pi}$ is not congruent to a unit modulo $\pi$. Hence, by Proposition 5, $F$ does not satisfy $(A_5)$ for $d = 11$ or $19$. 

The case $p = 7$. We checked that the natural map $Cl_F \to Cl_E$ is not trivial when $d = 6, 33, 195$. Hence, by Lemma 5, $F$ does not satisfy $(A_7)$ for these $d$. For $d = 5, 10, 115, 187$, the 2-part of $Cl_K$ is nontrivial and cyclic, and hence $F$ does not satisfy $(A_7)$ by Lemma 7. When $d = 13$, we found that $Cl_K = \mathbb{Z}/2^{53} \oplus \mathbb{Z}/3$ and $Cl_K^{S_F} \neq \{0\}$, and hence $F$ does not satisfy $(A_7)$. When $d = 19$, we found that $Cl_K = \mathbb{Z}/3$ and $Cl_K^{S_F} = \{0\}$. We checked that $F$ does not satisfy $(A_7)$ in this case similarly to the case where $p = 5$ and $d = 11, 19$. Finally, when $d = 3$, we found that $Cl_K = \{0\}$, and that $Cl_K(\pi)^{S_F} = \{0\}$ by Lemmas 9 and 10. Hence, $F$ satisfies $(A_7)$ for $d = 3$.

The case $p = 11$. For $d = 10, 35, 21, 30, 57, 85, 195, 435$ or 483, we found that the natural map $Cl_F \to Cl_E$ is not trivial. Hence, by Lemma 5, $F$ does not satisfy $(A_{11})$ for these $d$. For $d = 6, 13, 51, 123$ or 403, we have $h_E = 2$. Hence, by Lemma 7, $F$ does not satisfy $(A_{11})$ for these $d$. For $d = 43$, we have $h_F = 3$, and $F$ does not satisfy $(A_{11})$ by Lemma 8. Let us deal with the remaining cases where $d = 2, 7$ or 19. In these cases, we have $h_E = 1$. Instead of the field $K = F(\zeta_{11})$, we use the subfield $N = F(\cos 2\pi/11)$. We have $h_N = 5$ for $d = 2$ or 7, and $h_N = 55$ for $d = 19$. Let $\mathfrak{A}$ be an ideal of $N$. If $F$ satisfies $(A_{11})$, then $\mathfrak{A}^{12n_n}O_K = \alpha O_K$ for some $\alpha \in K^\times$ congruent modulo $\pi$ to a unit of $K$. Taking the norm to $N$, it follows that $\mathfrak{A}^{2n_n} = \beta O_N$. Here, $\beta = N_{K/N}\alpha$ and is congruent to a unit of $N$ modulo $\pi$. For these three $d$, we chose a nontrivial ideal $\mathfrak{A}$ of $N$ and checked that $\mathfrak{A}^{2n_n}$ is a principal ideal of $O_N$ and that its generator is not congruent to a unit of $N$ modulo $\pi$ after computing a system of fundamental units of $N$. Therefore, there exists no imaginary quadratic field satisfying $(A_{11})$. 

Observation/Question. Let $p$ be a prime number. As usual, we put $\tilde{p} = 4$ (resp. $p$) when $p = 2$ (resp. $p \geq 3$). We have seen that for the first five $\tilde{p}$, the number of imaginary quadratic fields $F$ satisfying $(A_p)$ is $4, 3, 2, 1$ and 0, respectively. What is the next term or a general term of this (arithmetic!) progression?

Remark 1. We can generalize Lemma 3 as follows. For a number field $F$, let $\mu_F$ be the group of roots of unity in $F$, and $\mu_F^1$, the subgroup of elements of odd order. Let $K/F$ be a finite cyclic extension with both $K$ and $F$ CM-fields. Assume that the following three conditions are satisfied:

(i) $2^e || [K : F]$ for some $e \geq 1$,
(ii) $\mu_F = \langle \zeta_{2^e} \rangle$,
(iii) there exists a prime ideal $\varphi$ of $F$ over an odd prime number $p$ such that $\varphi$ is totally ramified at the intermediate field $E$ of $K/F$ with $[E : F] = 2^e$.

By the last condition, we can write $E = F(a^{1/2^e})$ for some $a \in F^\times$ with $\text{ord}_\varphi(a) = 1$. Then we can show that the exponent of the kernel of the
natural map $Cl_F^{-} \rightarrow Cl_K^{-}$ divides 2 by an argument exactly similar to the proof of Lemma 3 using $\mu_K^1$ and $a^{1/2^e}$ in place of $\mu_p$ and $\sqrt{p^e}$.

**Remark 2.** If all imaginary abelian fields $K$ of degree 2$(p - 1)$ for which $\text{Cl}_{K}^{-h_p^p} = \{0\}$ were determined, it would be possible to determine all real quadratic fields satisfying $(A_p)$ for small primes $p$ by Proposition 6.

4. **Subfields of the $p$-cyclotomic field.** In this section, we deal with subfields of the $p$-cyclotomic field $\mathbb{Q}(\zeta_p)$. The following is an immediate consequence of Proposition 1. A more general statement is given in [9, Proposition 3.4].

**Proposition 8.** Let $p$ be an odd prime number. An imaginary subfield $F$ of $\mathbb{Q}(\zeta_p)$ satisfies $(A_p)$ if and only if $p = 3$ and $F = \mathbb{Q}(\zeta_3)$.

In the following, we summarize what is known or conjectured for the real case. Let $\mathcal{O}_F' = \mathcal{O}_F[1/p]$ be the ring of $p$-integers of $F$. We say that $F$ satisfies condition $(A'_p)$ if for any $\Gamma$-extension $N/F$, $\mathcal{O}_N'$ is cyclic over the group ring $\mathcal{O}_{F'}\Gamma$. It is known that if $F$ satisfies $(A_p)$ then it satisfies $(A'_p)$. Condition $(A'_p)$ is easier to handle than $(A_p)$, and many results on $(A'_p)$ are already obtained in [14, 16, 17, 18]. Let $K = F(\zeta_p)$. For instance, it is known that $F$ satisfies $(A'_p)$ if $h_K' = 1$, where $h_K'$ is the class number of the Dedekind domain $\mathcal{O}_K'$.

Let $K = \mathbb{Q}(\zeta_p)$, and $h_p$ the class number of $K$. As the unique prime ideal of $\mathcal{O}_K$ over $p$ is principal, we have $h_p = h_K'$. It is well known that $h_p = 1$ if and only if $p \leq 19$ (cf. [26, Theorem 11.1]). Hence, when $p \leq 19$, any subfield $F$ of $K = \mathbb{Q}(\zeta_p)$ satisfies $(A'_p)$. When $p \geq 23$, we proposed the following conjecture in [18].

**Conjecture 1.** Let $p$ be a prime number with $p \geq 23$, and $F$ a subfield of $\mathbb{Q}(\zeta_p)$ with $F \neq \mathbb{Q}$. If $[F : \mathbb{Q}] > 2$ or $p \equiv 1 \mod 4$, then $F$ does not satisfy condition $(A'_p)$ except when $p = 29$ and $[F : \mathbb{Q}] = 2$ or 7.

We have seen in [18, Proposition 4] that the conjecture is valid when $23 \leq p \leq 499$ and when $[K : F] \leq 4$ or $= 6$. A reason that the case $p = 29$ is exceptional is that $h_p^\pm$ is a power of 2 if and only if $p \leq 19$ or $p = 29$ by Horie [10]. When $p = 29$ and $[F : \mathbb{Q}] = 2$ or 7, it is known that $F$ satisfies $(A'_p)$ ([18, Proposition 4(II)]). In [16, Theorem 1], we determined all imaginary subfields $F$ of $\mathbb{Q}(\zeta_p)$ satisfying $(A'_p)$, and gave an affirmative answer to the conjecture for the imaginary case. In [17], we showed the following assertion for the real case.

**Proposition 9** ([17, Proposition 1]). Let $p \geq 23$. Assume that $q \parallel h_p^\pm$ for some odd prime number $q$. Then any real subfield $F$ of $\mathbb{Q}(\zeta_p)$ with $F \neq \mathbb{Q}$ does not satisfy $(A'_p)$. (Hence, it does not satisfy $(A_p)$.)
The assumption in this assertion is satisfied for all primes \( p \) with \( 23 \leq p < 2^{10} \) except \( p = 29, 31, 41 \) by the tables in [26], Lehmer and Masley [19] and Yamamura [28].

Now, we have enough reasons to propose the following:

**Conjecture 2.** A real subfield \( F \) of \( \mathbb{Q}(\zeta_p) \) with \( F \neq \mathbb{Q} \) does not satisfy \( (A_p) \) except when \( p \leq 19 \), or \( p = 29 \) and \( [F : \mathbb{Q}] = 2, 7 \).

Among the exceptional cases in Conjecture 2, we have checked that \( \mathbb{Q}(\sqrt{5}) \) satisfies \( (A_5) \) and that \( \mathbb{Q} \left( \cos \frac{2\pi}{7} \right) \) does not satisfy \( (A_7) \) by a computer calculation based upon Theorem 2. The difficult point is that the locally free class group \( Cl^0(\mathcal{O}_F \Gamma) \) is very complicated when \( F/\mathbb{Q} \) is ramified at \( p \).

**Acknowledgements.** The authors are grateful to the referee for carefully reading the original manuscript and for several kind suggestions. Thanks to the suggestions, we added Remark 1 and considerably improved the proof of Lemma 6. The first author was partially supported by Grant-in-Aid for Scientific Research (C), (No. 16540033), the Ministry of Education, Culture, Sports, Science and Technology of Japan. The second author was partially supported by Grant-in-Aid for Young Scientists (No. 16740019), the Ministry of Education, Culture, Sports, Science and Technology of Japan.

**References**

Quadratic fields satisfying the Hilbert–Speiser type condition


Faculty of Science
Ibaraki University
Bunkyo 2-1-1, Mito
Ibaraki, 310-8512, Japan
E-mail: hichimur@mx.ibaraki.ac.jp

Faculty and School of Engineering
The University of Tokushima
2-1, Minami-josanjima-cho
Tokushima, 770-8506, Japan
E-mail: hiroki@pm.tokushima-u.ac.jp

Received on 2.8.2006
and in revised form on 1.11.2006
(5253)