Note on class number parity of an abelian field of prime conductor, III

Humio Ichimura

Abstract

Let \( p \) be a prime number of the form \( p = 2\ell + 1 \) with some odd prime number \( \ell \). For such a prime number \( p \), it is shown that the relative class number \( h_p \) of the \( p \)-th cyclotomic field \( \mathbb{Q}(\zeta_p) \) is odd when 2 remains prime in \( \mathbb{Q}(\zeta_\ell) \) by Estes [3], Stevenhagen [11] and Metsänkylä [8] using a Bernoulli number associated to \( \mathbb{Q}(\zeta_p) \). In this note, we give an alternative proof of the assertion using a cyclotomic unit of \( \mathbb{Q}(\zeta_p)^+ \).

1. Introduction

For an odd prime number \( p \), let \( h_p^- \) denote the relative class number of the \( p \)-th cyclotomic field \( \mathbb{Q}(\zeta_p) \). Here, for an integer \( m \geq 1 \), \( \zeta_m \) is a primitive \( m \)-th root of unity. In this note, we deal with the case where \( p = 2\ell + 1 > 7 \) with an odd prime number \( \ell > 3 \). (When \( p = 7 \), it is known that \( h_7^- = 1 \).) For such a prime number \( p \), Davis [2] conjectured that \( h_p^- \) is always odd and showed that the conjecture is valid when 2 is a primitive root modulo \( \ell \). Estes [3] sharpened this result as follows.

Theorem 1. Let \( p = 2\ell + 1 \) be as above. Then \( h_p^- \) is odd when 2 remains prime in the maximal real subfield \( \mathbb{Q}(\zeta_\ell)^+ \) of \( \mathbb{Q}(\zeta_\ell) \).

The assumption on \( \ell \) in Theorem 1 is equivalent to saying that (I) 2 remains prime in the full cyclotomic field \( \mathbb{Q}(\zeta_\ell) \) or (II) \( \ell \equiv 7 \mod 8 \) and the decomposition field of the prime 2 in the extension \( \mathbb{Q}(\zeta_\ell)/\mathbb{Q} \) is \( \mathbb{Q}(\sqrt{-\ell}) \).

After Estes, Stevenhagen [11] and Metsänkylä [8] gave two different proofs of the theorem. These three proofs depend on the class number formula for \( h_p^- \) in terms of associated Bernoulli numbers (Washington [12, Theorem 4.17]) and make use of a Bernoulli number and the value \( \text{ord}_3(p + 1) \). Here, for a prime number \( q \), \( \text{ord}_q(*) \) denotes the additive valuation on the rationals \( \mathbb{Q} \) with \( \text{ord}_q(q) = 1 \).

In this note, we give an alternative proof of Theorem 1 using a cyclotomic unit of \( \mathbb{Q}(\zeta_p)^+ \) and the value \( \text{ord}_2(p + 1) \). We effectively use a polynomial over the finite field...
Remark 1. For a prime number \( p \), let \( h_p^+ \) be the class number of \( \mathbb{Q}(\zeta_p)^+ \). It is well known that \( h_p^+ \) is odd if \( h_p \) is odd ([12, Theorem 10.2]). Therefore, when \( p = 2\ell + 1 \), it follows from Theorem 1 that \( h_p^+ \) is odd under the same assumption on \( \ell \). Recently, for a fixed integer \( n \geq 2 \), this type of assertions are obtained also for a prime number \( p \) of the form \( p = 2n\ell + 1 \) and the class number of the real subfield of \( \mathbb{Q}(\zeta_p) \) of degree \( \ell \), where \( \ell \) is an odd prime number ([7, Theorems 2, 3]).

2. Cyclotomic units

In this section, we prepare some lemmas on cyclotomic units. For a while, \( p \) denotes a general odd prime number. Let \( 2^{e+1} \) be the highest power of 2 dividing \( p-1 \). Namely, \( e+1 = \text{ord}_2(p-1) \). Let \( K = \mathbb{Q}(\zeta_p) \), and let \( k \) be the imaginary subfield of \( K \) of degree \( 2^{e+1} \) and \( F \) the real subfield of \( K \) of degree \( (p-1)/2^{e+1} \). Then we have \( K = FK \), and we can naturally identify the Galois group \( \Delta = \text{Gal}(F/\mathbb{Q}) \) with \( \text{Gal}(K/k) \). For an abelian field \( N \), we denote by \( A_N \) (resp. \( \tilde{A}_N \)) the 2-part of the ideal class group of \( N \) in the usual sense (resp. in the narrow sense). When \( N \) is an imaginary abelian field, \( A_N^+ \) denotes the kernel of the norm map \( A_N \to A_{N^+} \), where \( N^+ \) is the maximal real subfield of \( N \). Let \( C = CF \) be the group of cyclotomic units of \( F \) in the sense of Sinnott [10] (the one denoted by \( C_1 \) in [10, page 209]). The groups \( A_K^+, A_F, C/C^2 \) are naturally regarded as modules over the group ring \( \mathbb{Z}_2[\Delta] \) where \( \mathbb{Z}_2 \) is the ring of 2-adic integers.

Let \( \chi \) be a \( \mathbb{Q}_2 \)-valued character of \( \Delta \), and let

\[
e_\chi = \frac{1}{|\Delta|} \sum_{\delta \in \Delta} \text{Tr}_{\mathbb{Q}_2(\chi)/\mathbb{Q}_2}(\chi(\delta))\delta^{-1}
\]

be the associated idempotent of the group ring \( \mathbb{Z}_2[\Delta] \). Here, \( \mathbb{Q}_2 \) is a fixed algebraic closure of the 2-adic rationals \( \mathbb{Q}_2 \). \( \mathbb{Q}_2(\chi) \) is the subfield of \( \mathbb{Q}_2 \) generated by the values of \( \chi \) over \( \mathbb{Q}_2 \), and \( \text{Tr} \) denotes the trace map. The subring \( e_\chi \mathbb{Z}_2[\Delta] \) of \( \mathbb{Z}_2[\Delta] \) is identified with the integer ring \( \mathcal{O}_\chi \) of \( \mathbb{Q}_2(\chi) \) by \( e_\chi \delta \leftrightarrow \chi(\delta) \) (\( \delta \in \Delta \)). For a module \( M \overline{\mathbb{Z}_2}[\Delta] \) (such as \( A_K^+, C/C^2 \)), let \( M(\chi) = M^{e_\chi} \) (or \( e_\chi M \)) be the \( \chi \)-part of \( M \). Then, by the above identification, we can naturally regard \( M(\chi) \) as a module over \( \mathcal{O}_\chi \).

For a real number \( x \in \mathbb{R}^\times \), we put \( \iota(x) = 0 \) or 1 according as \( x > 0 \) or \( x < 0 \). Fixing an embedding \( F \to \mathbb{R} \), we define the signature map \( \varphi_F \) on \( F^\times \) by

\[
\varphi_F : F^\times \to \mathbb{F}_2[\Delta], \quad x \to \sum_{\delta \in \Delta} \iota(\delta(x))\delta^{-1},
\]

which is compatible with the natural action of \( \Delta \). The map \( \varphi_F \) induces the signature map \( \varphi_C : C/C^2 \to \mathbb{F}_2[\Delta] \) on the group of cyclotomic units \( C \). We denote by \( \varphi_\chi \) the restriction of \( \varphi_C \) to the \( \chi \)-part \( (C/C^2)(\chi) \);

\[
\varphi_\chi : (C/C^2)(\chi) \to \mathbb{F}_2[\Delta](\chi) = \mathcal{O}_\chi/2\mathcal{O}_\chi, \quad [\epsilon] \to \sum_{\delta \in \Delta} \iota(\delta(\epsilon))\chi(\delta)^{-1}.
\]
Here, \([\epsilon]\) is the class in \(C/C^2\) represented by a unit \(\epsilon \in C\).

Let \(\xi\) be a \(Q_2\)-valued Dirichlet character of conductor \(p\) and order \(2^{e+1}\). We naturally regard a character \(\chi\) of \(\Delta\) as a Dirichlet character. Then \(\xi \chi\) is an odd Dirichlet character of conductor \(p\). We denote by

\[
\beta_{\chi} = \frac{1}{2} B_{1,\xi} = \frac{1}{2p} \sum_{a=1}^{p-1} a(\xi \chi)(a) \in \bar{Q}_2
\]

the half of the generalized Bernoulli number. It is known that \(\beta_{\chi}\) is a 2-adic integer when \(\chi\) is nontrivial (Hasse [5, Satz 32]).

**Lemma 1.** Under the above setting, let \(\chi\) be a nontrivial \(Q_2\)-valued character of \(\Delta\). Then the following three conditions are equivalent with each other.

(i) \(A_F(\chi) = \{0\}\).

(ii) \(\beta_{\chi^{-1}}\) is a 2-adic unit in \(\bar{Q}_2\).

(iii) The signature map \(\varphi_{\chi}\) is surjective.

**Proof.** The equivalence (i) \(\Leftrightarrow\) (ii) follows from Greither [4, Theorem A], which is a consequence of the Iwasawa main conjecture. The condition (i) holds if and only if the narrow class group \(\tilde{\mathcal{A}}_{K^+}(\chi)\) is trivial by [6, Theorem 2]. The last condition is equivalent to \(\tilde{\mathcal{A}}_F(\chi) = \{0\}\) because the cyclic extension \(K^+/F\) of degree \(2^e\) is unramified outside the unique prime ideal over \(p\) (see [12, Theorem 10.4]). Let \(E\) be the group of global units of \(F\). Let \(F_{>0}\) be the totally positive elements of \(F^\times\), and set \(E^+ = E \cap F_{>0}\). We see that

\[
(E/E^2)(\chi) \cong \mathcal{O}_\chi/2\mathcal{O}_\chi
\]  

(2.1)

as \(\mathcal{O}_\chi\)-modules by a theorem of Minkowski on units of a Galois extension over \(Q\) (Narkiewicz [9, Theorem 3.26]). As \(E^2 \subseteq E^+\), it follows from (2.1) that \((E/E^+)(\chi)\) is trivial or isomorphic to \(\mathcal{O}_\chi/2\mathcal{O}_\chi\). We see that \(A_F(\chi) = \{0\}\) if and only if (a) \(A_F(\chi) = \{0\}\) and (b) \((E/E^+)(\chi) \cong \mathcal{O}_\chi/2\mathcal{O}_\chi\) because of the exact sequence

\[
\{0\} \to F^\times/EF_{>0} \to \tilde{A}_F \to A_F \to \{0\}.
\]

The condition (a) is equivalent to \((a') (E/C)(\chi) = \{0\}\) by Cornacchia and Greither [1, Proposition 10], which is a consequence of the Iwasawa main conjecture. Using (2.1), we see that the conditions (a') and (b) hold if and only if the condition (iii) holds. Therefore, we obtain the equivalence (i) \(\Leftrightarrow\) (iii). \(\square\)

In the following, \(p\) denotes an odd prime number of the form \(p = 2\ell + 1\) with an odd prime number \(\ell\). Let \(K = Q(\zeta_p)\) and let \(F = K^+\) be the maximal real subfield of \(K\). For each \(1 \leq a \leq \ell\), we denote by \(\sigma_a\) the restriction to \(F\) of the automorphism of \(K\) sending \(\zeta_p^a\). Then we have

\[
\Delta = \text{Gal}(F/Q) = \{\sigma_a \mid 1 \leq a \leq \ell\}.
\]

As a primitive \(p\)th root of unity, we choose and fix \(\zeta_p = \exp(2\pi\sqrt{-1}/p)\). We put

\[
\epsilon_1 = \zeta_p + \zeta_p^{-1} = 2\cos(2\pi/p) \quad \text{and} \quad \epsilon_2 = \zeta_p + 1 + \zeta_p^{-1} = 2\cos(2\pi/p) + 1.
\]
These are cyclotomic units of \( F \). Under the notation in [12, §8.1], we have \( \epsilon_1 = \sigma_2(\xi_2) \) and \( \epsilon_2 = \xi_3 \). We see that \( 2 \) or \( p - 2 \) is a primitive root modulo \( p \) as \( 2^2 \not\equiv 1 \mod p \). Using this fact, we see from [12, Lemma 8.1] that \( -1 \) and \( \epsilon_1 \) generate the group \( C = C_F \) of cyclotomic units of \( F \) over \( \mathbb{Z}[\Delta] \). Further, we put

\[
\eta = \epsilon_1 \epsilon_2^{-1} (\in C).
\]

Since \( 0 < 2\pi a/p < \pi \), we see that \( \sigma_a(\epsilon_1) = 2 \cos(2\pi a/p) < 0 \) if and only if \( \pi/2 < 2\pi a/p < \pi \); namely if and only if \( p/4 < a < p/2 \). Similarly, we see that \( \sigma_a(\epsilon_2) < 0 \) if and only if \( p/3 < a < p/2 \). Thus we obtain

\[
\varphi_F(\epsilon_1) = \sum_{p/4 < a < p/2} \sigma_a^{-1} \quad \text{and} \quad \varphi_F(\epsilon_2) = \sum_{p/3 < a < p/2} \sigma_a^{-1}.
\]

(2.2)

It follows that

\[
\varphi_F(\eta) = \sum_{p/4 < a < p/3} \sigma_a^{-1}.
\]

(2.3)

We put

\[
\alpha_\chi := \sum_{p/4 < a < p/3} \chi(a) \in \mathcal{O}_\chi/2\mathcal{O}_\chi.
\]

(2.4)

\[\text{Lemma 2.} \quad \text{Let } \chi \text{ be a nontrivial } \mathbb{Q}_2 \text{-valued character of } \Delta. \text{ If } A_K^{-}(\chi^{-1}) \text{ is nontrivial, then } \alpha_\chi = 0 \text{ in } \mathcal{O}_\chi/2\mathcal{O}_\chi.\]

\[\text{Proof.} \quad \text{If } A_K^{-}(\chi^{-1}) \text{ is nontrivial, then by Lemma 1, the signature map } \varphi_{\chi^{-1}} \text{ on } (C/C^2)(\chi^{-1}) \text{ is the zero-map. Hence, it follows from (2.3) that } \alpha_\chi = \varphi_{\chi^{-1}}([\eta]) = 0. \quad \square \]

\[\text{Remark 2.} \quad \text{In Lemma 1, the equivalence } (\text{ii}) \Leftrightarrow (\text{iii}) \text{ is obtained from two consequences of the Iwasawa main conjecture; the one for } A_K^{-} \text{ and the other for } A_F. \text{ However, when } p = 2\ell + 1, \text{ the equivalence is shown in quite an elementary way. Actually, as } \epsilon_1 \text{ and } -1 \text{ generate } C \text{ over } \mathbb{Z}[\Delta], \text{ we see from (2.2) that } \varphi_\chi \text{ is surjective if and only if}
\]

\[
\sum_{p/4 < a < p/2} \chi^{-1}(a) \in (\mathcal{O}_\chi/2\mathcal{O}_\chi)^\times.
\]

This is equivalent to

\[
\sum_{1 \leq a < p/4} \chi^{-1}(a) = \sum_{a=1}^{(\ell-1)/2} \chi^{-1}(a) \in (\mathcal{O}_\chi/2\mathcal{O}_\chi)^\times
\]

(2.5)

because the sum of the values \( \chi^{-1}(a) \) for all \( 1 \leq a \leq \ell = (p - 1)/2 \) vanishes. On the other hand, it is shown in [11, page 776] that the condition (ii) on \( \beta_{\chi^{-1}} \) is equivalent to (2.5) in an elementary way.
3. Proof of Theorem 1

We let \( p = 2\ell + 1 \) (\( > 7 \)), and we use the same notation as in the previous sections. In what follows, we assume that 2 remains prime in \( \mathbb{Q}(\zeta_\ell)^+ \). As we mentioned just after Theorem 1, the assumption is equivalent to saying that (I) 2 remains prime in \( \mathbb{Q}(\zeta_\ell) \) or (II) \( \ell \equiv 7 \mod 8 \) and the decomposition field of the prime 2 in \( \mathbb{Q}(\zeta_\ell)/\mathbb{Q} \) is \( \mathbb{Q}(\sqrt{-\ell}) \). We choose and fix a complete set \( \Omega_F \) of representatives of the nontrivial \( \mathbb{Q}_2 \)-valued characters of \( \Delta \). We see that the condition (I) (resp. (II)) holds if and only if \( \Omega_F = \{ \chi \} \) (resp. \( \Omega_F = \{ \chi, \chi^{-1} \} \)) for some \( \chi \). We see that

\[
A_K^\omega = A_K(\chi) \quad \text{or} \quad A_K = A_K(\chi) \oplus A_K(\chi^{-1})
\]

according as \( \Omega_F = \{ \chi \} \) or \( \{ \chi, \chi^{-1} \} \). This is because, for the trivial character \( \chi_0 \) of \( \Delta \), the \( \chi_0 \)-part \( A_K(\chi_0) = A_{\mathbb{Q}(\sqrt{-\ell})} \) is trivial.

**Proof of Theorem 1 for the case (I).** In this case, since \( \mathbb{Q}_2(\chi) = \mathbb{Q}_2(\zeta_\ell) \) is of degree \( \ell + 1 > 7 \) is a prime number. In particular, we see that \( \chi_0 \equiv -1 \mod p \). We put \( \zeta_\ell = \chi(-2) \), which is a primitive \( \ell \)-th root of unity in \( \mathbb{Q}_2 \). Then we see that

\[
\chi(a) = \zeta_\ell^{\lambda(a)}.
\]

In view of (2.4), we define polynomials \( f(T) \) and \( \tilde{f}(T) \) in \( \mathbb{F}_2[T] \) by

\[
f(T) = \sum_{p/4 \leq a < p/3} T^{\lambda(a)} \quad \text{and} \quad \tilde{f}(T) = T^{\ell} f(1/T) = \sum_{p/4 < b < p/3} T^{\ell-\lambda(b)},
\]

and we put

\[
g(T) = f(T) \tilde{f}(T) = \sum_{a,b} T^{\lambda(a)+\ell-\lambda(b)} \in \mathbb{F}_2[T]
\]
where $a$ and $b$ run over the integers with
\[ \frac{p}{4} < a, b < \frac{p}{3}. \tag{3.5} \]

Now assume that $A^K$ is nontrivial. Then it follows from (3.1) and Lemma 2 that
\[ \alpha \alpha^{-1} = 0 \text{ in } O_x/2O_x. \tag{3.6} \]
By (2.4) and (3.4), this implies that $\zeta_{\ell} = \chi(-2)$ and $\zeta_{\ell}^{-1} = \chi^{-1}(-2)$ are roots of the polynomial $g(T)$. Then, because of the condition (II), we observe that $g(T)$ is a multiple of the $\ell$th cyclotomic polynomial $\Phi_{\ell}(T)$ in $\mathbb{F}_2[T]$. Further, using (3.2), we see that $f(1) = (p+1)/12 = 0$ in $\mathbb{F}_2$. Therefore, it follows that $g(T)$ is a multiple of $T^{\ell} - 1$ in $\mathbb{F}_2[T]$. For $0 \leq r \leq \ell - 1$, we define a set $X_r$ by
\[ X_r = \{ (a, b) \mid p/4 < a, b < p/3, \lambda(a) \equiv \lambda(b) + r \mod \ell \}, \]
and we let $c_r$ be the cardinality of $X_r$; $c_r = |X_r|$. Then we see that the polynomial
\[ h(T) = \sum_{r=0}^{\ell-1} c_r T^r \in \mathbb{F}_2[T] \]
is congruent to $g(T)$ modulo $T^{\ell} - 1$. From the above, we obtain the following lemma.

**Lemma 3.** Under the above setting, the congruence
\[ c_0 \equiv c_1 \equiv \cdots \equiv c_{\ell-1} \equiv 0 \pmod{2} \]
would hold if $h_p^\ell$ were even.

We put $s = \text{ord}_2(\ell+1) - 1$. We have $s + 2 = \text{ord}_2(p+1)$ as $p = 2\ell + 1$, and $s \geq 2$ by (3.2). On the integer $c_r$, we show the following:

**Theorem 2.** Under the above setting, the following congruences hold.
\[ c_0 \equiv c_1 \equiv \cdots \equiv c_s \equiv 0 \pmod{2} \quad \text{but} \quad c_s \equiv 1 \pmod{2}. \]

**Proof of Theorem 1 for the case (II).** We obtain Theorem 1 for the case (II) immediately from Lemma 3 and Theorem 2. \hfill \square

Let $t$ be an integer with $2 \leq t \leq s = \text{ord}_2(\ell+1) - 1$. Then, by (3.2), we can write
\[ \ell = 3 \cdot 2^{t+1} \cdot m_t - 1 \quad \text{and} \quad p = 3 \cdot 2^{t+2} \cdot m_t - 1 \tag{3.7} \]
for some integer $m_t \geq 1$. We let $\omega_t = 1$ or 2 according as $t$ is even or odd, and we put
\[ \phi_t = \frac{2^{t-2} - \omega_t}{3} - 1 \in \mathbb{Z}. \]
On the coefficients $c_r$ of the polynomial $h(T)$, we show the following lemma.
Lemma 4. (i) \( c_0 = (p + 1)/12 \) and \( c_1 = 0 \).
(ii) For \( t \) with \( 2 \leq t \leq s \), \( c_t = (2\phi_t + 3)m_t \).

Proof of Theorem 2. By Lemma 4 and (3.2), \( c_0 \equiv c_1 \equiv 0 \mod 2 \). Let \( 2 \leq t \leq s \). As \( s + 1 = \text{ord}_2(\ell + 1) \), we see from (3.7) that \( m_t \) is even for \( t < s \) and \( m_s \) is odd. Therefore, it follows from Lemma 4 that \( c_t \equiv 0 \mod 2 \) for \( 2 \leq t < s \) and \( c_s \equiv 1 \mod 2 \). Thus we obtain the assertion. \( \square \)

Proof of Lemma 4. We let \( t \geq 4 \) and show the assertion (ii). The assertion (ii) for \( t = 2, 3 \) and the assertion (i) are shown similarly and more easily. We count the number of pairs \( (a, b) \) satisfying the inequality (3.5) for which \( (a) + (b) + t \mod \ell \).

Because of (3.3), the last condition is equivalent to \( a \equiv s_p(2^t b) \) or \( a \equiv p - s_p(2^t b) \mod p \). This is equivalent to

\[
a = s_p(2^t b) \quad \text{or} \quad a = p - s_p(2^t b). \tag{3.8}
\]

Because of (3.5), we see that \( 2^t b \) is contained in the interval

\[
2^{t-2}p \leq 2^t b < 2^t \times \frac{p}{3}.
\]

This interval for \( 2^t b \) is divided into the following two types of short intervals of length \( \leq p \):

(A) \( (2^{t-2} + k)p \leq 2^t b \leq (2^{t-2} + k + 1)p - 1 \),

for \( 0 \leq k \leq \phi_t \), and

(B) \( \frac{2^t - \omega_t}{3} p \leq 2^t b < \frac{2^t - \omega_t}{3} p + \frac{\omega_t}{3} p \).

Here, note that

\[
2^{t-2} + \phi_t + 1 = \frac{2^t - \omega_t}{3}.
\]

Further, the condition \( t \geq 4 \) is used to assure \( \phi_t \geq 0 \). From (3.7), it follows that

\[
\frac{p}{2^t} = 12m_t - \frac{1}{2^t}. \tag{3.9}
\]

First, we deal with the interval (A)\(_k\). We put \( x_k(b) = 2^t b - (2^{t-2} + k)p \) so that we have \( s_p(2^t b) = x_k(b) \) for those \( b \) satisfying (A)\(_k\). We see that an integer \( b \) satisfies (A)\(_k\) when \( x_k(b) \) or \( p - x_k(b) \) lies in the interval (3.5). Hence, in view of (3.8), it suffices to count the number of those \( b \) for which \( x_k(b) \) or \( p - x_k(b) \) lies in (3.5). Using (3.9), we see easily that \( x_k(b) \) lies in the interval (3.5) if and only if

\[
(3 \cdot 2^t + 12k + 3)m_t \leq b \leq (3 \cdot 2^t + 12k + 4)m_t - 1
\]

and that \( p - x_k(b) \) lies in (3.5) if and only if

\[
(3 \cdot 2^t + 12k + 8)m_t \leq b \leq (3 \cdot 2^t + 12k + 9)m_t - 1.
\]
Therefore, we obtain $2m_t$ pairs $(a, b)$ from $(A)_k$ satisfying (3.5) and $\lambda(a) \equiv \lambda(b) + t \mod \ell$ for each $0 \leq k \leq \phi_t$.

Next, let us deal with the interval (B). We put

$$y(b) = 2^t b - \frac{2^t - \omega_t}{3} p.$$  

Then, we have

$$0 \leq s_p(2^t b) = y(b) < \frac{\omega_t}{3} p$$

for those $b$ satisfying (B). It follows that $p - y(b) > p/3$, and hence $p - y(b)$ does not lie in (3.5). We see that an integer $b$ satisfies (B) when $y(b)$ lies in (3.5). Using (3.9), we see that $y(b)$ lies in (3.5) if and only if

$$(4(2^t - \omega_t) + 3)m_t \leq b \leq (4(2^t - \omega_t) + 4)m_t - 1.$$  

Thus, we obtain $m_t$ pairs $(a, b)$ from (B).

Now we obtain

$$(2(1 + \phi_t) + 1)m_t = (2\phi_t + 3)m_t$$

pairs $(a, b)$ satisfying the desired conditions from the intervals $(A)_k$ with $0 \leq k \leq \phi_t$ and (B).

**Remark 3.** We showed Theorem 1 by using the cyclotomic unit $\eta = \epsilon_1\epsilon_2^{-1}$. We can use other cyclotomic units to show the theorem. For instance, let us use the cyclotomic unit $\epsilon_1$. Then the element of $\mathcal{O}_\chi/2\mathcal{O}_\chi$ corresponding to $\alpha_\chi$ is

$$\gamma_\chi = \sum_{1 \leq a < p/4} \chi(a).$$

For this, see (2.5) in Remark 2. Similarly to the assertion (3.6) for the unit $\eta$, we can show that $\gamma_\chi \gamma_{\chi^{-1}} = 0$ in $\mathcal{O}_\chi/2\mathcal{O}_\chi$ if $h_\chi$ were even under the condition (II) of Theorem 1. For each $0 \leq r \leq \ell - 1$, let $d_r$ be the number of pairs $(a, b)$ such that $1 \leq a, b < p/4$ and $\lambda(a) \equiv \lambda(b) + r \mod \ell$. Then the polynomial corresponding to $h(T)$ is

$$j(T) = \sum_{r=0}^{\ell-1} d_r T^r \in \mathbb{F}_2[T].$$

This polynomial coincides with the one which was used in [11, page 777] to show Theorem 1 for the case (II). In [11], the polynomial $j(T)$ was obtained from the Bernoulli number $\beta_\chi$. It seems interesting that the same polynomial appears from the two different directions.

**Remark 4.** The condition $\lambda(a) \equiv \lambda(b) + r \mod \ell$ is equivalent to $a \equiv \pm 2^t b \mod p$, and the condition $\lambda(a) \equiv \lambda(b) + (\ell - r) \mod \ell$ is equivalent to $b \equiv \pm 2^t a \mod p$. Using this fact, we easily see that $c_r = c_{\ell-r}$ and $d_r = d_{\ell-r}$ for each $1 \leq r \leq \ell - 1$. The integer $c_0$ is even by Lemma 4. We easily see that $d_0 = (p - 3)/4$ is odd. (For this, see also
In particular, it follows that the polynomials $h(T)$ and $j(T)$ over $\mathbb{F}_2$ satisfy
\[ T^\ell h(1/T) = h(T) \quad \text{and} \quad T^\ell (j(1/T) - 1) = j(T) - 1, \]
respectively. For example, when $p = 47 = 2 \cdot 23 + 1$, $h(T)$ and $j(T) - 1$ equal
\[ T^2 + T^6 + T^7 + T^9 + T^{14} + T^{16} + T^{17} + T^{21} \]
and
\[ T + T^2 + T^3 + T^4 + T^5 + T^6 + T^{10} + T^{11} + T^{17} + T^{18} + T^{19} + T^{20} + T^{21} + T^{22}, \]
respectively.

**Added in Proof.** In §3, we showed that the signature map $\varphi_C$ is surjective under the assumption of Theorem 1. Recently, we noticed that this assertion is already obtained in the paper of M.-H. Kim and S.-G. Lim entitled “Square classes of totally positive units”, J. Number Theory, 125 (2007), 1–6. They use a polynomial associated to the signature of the cyclotomic unit $-\epsilon_2$. Our treatment of the polynomial $h(T)$ is similar to theirs.

**References**

[1] P. Cornacchia and C. Greither, Fitting ideals of class groups of real fields of prime power conductor, J. Number Theory, 73 (1998), no. 2, 459–471.

[2] D. Davis, Computing the number of totally positive circular units which are square, J. Number Theory, 10 (1978), no. 1, 1–9.

[3] D. R. Estes, On the parity of the class number of the field of $q$th roots of unity, Rocky Mount. J. Math., 19 (1989), no. 3, 675–682.

[4] C. Greither, Class groups of abelian fields and the main conjecture, Ann. Inst. Fourier, 42 (1992), no. 3, 449–499.

[5] H. Hasse, Über die Klassenzahl abelscher Zahlkörper, Akademia Verlag, Berlin, 1952. Reprinted with an introduction by J. Martine; Springer, Berlin, 1985.

[6] H. Ichimura, Class number parity of a quadratic twist of a cyclotomic field of prime power conductor, Osaka J. Math., 50 (2013), no. 2, 563–572.

[7] H. Ichimura, Note on the class number parity of an abelian field of prime conductor, II, Kodai Math. J., 42 (2019), no. 1, 99–110.

[8] T. Metsänkylä, Some divisibility results for the cyclotomic class number, Tatra Mt. Math. Publ., 11 (1997), 59–68.

[9] W. Narkiewicz, Elementary and Analytic Theory of Algebraic Numbers (3rd ed.), Springer, Berlin, 2004.
[10] W. Sinnott, On the Stickelberger ideal and the circular units of an abelian field, Invent. Math., 62 (1980), no. 2, 181–234.

[11] P. Stevenhagen, Class number parity of the $p$th cyclotomic field, Math. Comp., 63 (1994), no. 208, 773–784.

[12] L. C. Washington, Introduction to Cyclotomic Fields (2nd ed.), Springer, New York, 1997.