ACTA ARITHMETICA
LXVI.4 (1994)

Some remarks about the power residue symbol

by

J. Wójcik

1. Introduction. Let K be an algebraic number field with $\zeta_m \in K$, $\zeta_m = e^{2\pi i/m}$. Denote by O_K the ring of integers of K. If $\alpha \in O_K \setminus \{0\}$ and A is an ideal of O_K prime to $m\alpha$ then $\left(\frac{\alpha|K}{A}\right)_m$ denotes the mth power residue symbol. It is known that if a, b are rational integers different from zero and b is prime to $3a$ or $2a$ then $(a/b)_3 = 1$ or $(a/b)_4 = 1$ respectively.

On the other hand, H. Hasse gives in [1], p. 65, the following result: if k is an algebraic number field, $\zeta_m \in k$, $a, b \in \mathbb{Z} \setminus \{0\}$ and $(b, ma) = 1$ then

$$\left(\frac{a\,|\,k}{b}\right)_m = (\pm 1)^g, \quad \text{where} \quad g = [k : P_m],\ P_m = \mathbb{Q}(\zeta_m).$$

It turns out that the above result can be refined. Namely, if the case $m = 2$ and $[k : \mathbb{Q}]$ odd is excluded then we always have

$$\left(\frac{a\,|\,k}{b}\right)_m = 1. \tag{1}$$

Let k, K be algebraic number fields such that $k \subseteq K$, and $\zeta_m \in K$. The main aim of the present paper is to give necessary and sufficient conditions for the equality

$$\left(\frac{\alpha\,|\,K}{A}\right)_m = 1 \tag{2}$$

to hold, where α is a number (different from zero) and A is an ideal of O_k prime to $m\alpha$.

It is known that the extension $K(\sqrt[m]{\alpha})/K$ is the class field corresponding to the group of ideals A of O_K prime to $m\alpha$ and such that $\left(\frac{\alpha|K}{A}\right)_m = 1$. (2) means that any ideal of O_k prime to $m\alpha$ treated as an ideal of O_K belongs to the principal class.

Notation. m denotes a positive integer. Let k be an algebraic number field. Put $k_m = k(\zeta_m)$ and let $N_m = N_{k_m/\mathbb{Q}}$, $N = N_{k/\mathbb{Q}}$ denote the absolute norms in k_m, k respectively. For $a \in \mathbb{Z}$, $\overline{a}$ denotes the residue class $\bmod\, m$ containing a. Let G be any subgroup of the multiplicative group of residue classes $\bmod\, m$. Let $d \mid m$. Then $G_d = G_d(m)$ denotes the subgroup of those residue classes $\bmod\, m$ of G which are congruent to 1 mod m/d.

We shall show

THEOREM 1. *Let k, K be algebraic number fields such that $k \subseteq K$ and $\zeta_m \in K$. Let n denote the number of roots of unity of degree m contained in k. Let $2^\nu \parallel m$ $(\nu \ge 0)$ and*

$$n' = \begin{cases} n & \text{if } n \not\equiv 2 \bmod 4 \text{ or } m \not\equiv 0 \bmod 4, \\ n/2 & \text{otherwise.} \end{cases}$$

Moreover, let $m = m'm''$, where $(m', n') = 1$ and m'' contains only prime factors dividing n'. Further, let $m' = 2^\mu m'''$ $(\mu \ge 0)$, $2 \nmid m'''$, $bm' \equiv (m', n) \bmod n$, $(b, n) = 1$. Finally, let $\alpha \in O_k \setminus \{0\}$, and A be an ideal of O_k prime to $m\alpha$. Then

$$(3)\qquad \left(\frac{\alpha \mid K}{A}\right)_m = \begin{cases} \left(\frac{\alpha|K}{A}\right)_n^{b[K:k_{m''}]} & \text{if } \operatorname{ord}_2 n = \operatorname{ord}_2 m \\ & \text{or } [K : k_{m''2^\mu}] \equiv 0 \bmod 2 \\ & \text{or the field } k \cap P_{2^\nu} \text{ is real,} \\ \left(\frac{\alpha|K}{A}\right)_n^{b[K:k_{m''}]+n/2} & \text{otherwise.} \end{cases}$$

THEOREM 2. *Under the notation of Theorem 1, in order that*

$$(4)\qquad \left(\frac{\alpha \mid K}{A}\right)_m = 1$$

for every $\alpha \in O_k \setminus \{0\}$ and every ideal A of O_k prime to $m\alpha$, it is necessary and sufficient that the following two conditions hold:

(i) *either* $\operatorname{ord}_2 n = \operatorname{ord}_2 m$ *or* $[K : k_{m''2^\mu}] \equiv 0 \bmod 2$ *or the field* $k \cap P_{2^\nu}$ *is real,*

(ii) $[K : k_{m''}] \equiv 0 \bmod n$.

COROLLARY. *Let K be an algebraic number field. Assume that $\zeta_m \in K$. Let $a, b \in \mathbb{Z} \setminus \{0\}$ with $(b, ma) = 1$. Then*

$$\left(\frac{\alpha \mid K}{b}\right)_m = 1$$

except the case when $m = 2$ and the field K is of an odd degree.

2. Preliminaries. First we shall prove five lemmas.

LEMMA 1. *Let m be a positive integer and G be a subgroup of the multiplicative group of residue classes* mod m *prime to m, say $G = \{\overline{a}_1, \ldots, \overline{a}_t\}$, $a_j \in \mathbb{Z}$, $(a_j, m) = 1$. Put $l = (a_1 - 1, \ldots, a_t - 1, m)$ and $S = \sum_{j=1}^t a_j$. Let*

$2^\nu \parallel m$ $(\nu \ge 0)$ *and*

$$l' = \begin{cases} l & \text{if } l \not\equiv 2 \bmod 4 \text{ or } m \not\equiv 0 \bmod 4, \\ l/2 & \text{otherwise.} \end{cases}$$

Moreover, let $m = k'k''$, *where* $(k', l') = 1$ *and* k'' *contains only prime factors dividing* l'. *Further, let* $k' = 2^\kappa k'''$ $(\kappa \ge 0)$, $2 \nmid k'''$, $ak' \equiv (k', l) \bmod l$, $(a, l) = 1$. *Then*

$$S \equiv 0 \bmod k'''.$$

Proof. Let $p^r \parallel k'''$, p a prime, $r > 0$. Hence $p > 2$. Since k' and l' are relatively prime we have

$$p \nmid l. \tag{5}$$

Let g be a primitive root $\bmod p^r$. Set $H = G_{m/p^r}$. The quotient group G/H is isomorphic to some subgroup of the multiplicative group of residue classes $\bmod p^r$. Hence $G/H = \{g^{ju}H : j = 0, 1, \ldots, v-1\}$ where $uv = \varphi(p^r) = (p-1)p^{r-1}$.

We have

$$g^u \not\equiv 1 \bmod p. \tag{6}$$

Otherwise we would have $a_j \equiv 1 \bmod p$ for every j and $p \mid l$, contrary to (5).

By (6) and Euler's theorem,

$$S \equiv |H| \sum_{j=0}^{v-1} g^{ju} = |H| \frac{g^{\varphi(p^r)} - 1}{g^u - 1} \equiv 0 \bmod p^r.$$

Hence $S \equiv 0 \bmod k'''$. ∎

LEMMA 2. *Let* $l \equiv 2 \bmod 4$ *and* $m \equiv 0 \bmod 4$. *Then*

$$|G_{k'''}| \equiv |G_{k'''k''}| \bmod 2, \qquad |G_{k'}| \equiv 0 \bmod 2.$$

Proof. We have $\kappa = \nu \ge 2$. According to the definition of l and by the Lemma of [2] (p. 218) the quotient group $G/G_{k'}$ is of order k''/l'. Since in this case $k'' \equiv 1 \bmod 2$ we have

$$[G : G_{k'}] \equiv 1 \bmod 2. \tag{7}$$

Set $H = G_{k'''k''}$. We have $G_{k'''} = H \cap G_{k'}$ and $H/G_{k'''} = H/H \cap G_{k'} \cong HG_{k'}/G_{k'} \subseteq G/G_{k'}$. Hence by (7), $[H : G_{k'''}] \equiv 1 \bmod 2$ and

$$|H| = [H : G_{k'''}]|G_{k'''}| \equiv |G_{k'''}| \bmod 2. \tag{8}$$

The order of the quotient group G/H is a power of two. This power is not trivial. Otherwise we would have $a_j \equiv 1 \bmod 2^\nu$ for each j and $l \equiv 0 \bmod 4$, contrary to the assumption. Thus we have $|G| \equiv 0 \bmod 2$. Further, $|G| = [G : G_{k'}]|G_{k'}|$ and by (7),

$$|G_{k'}| \equiv 0 \bmod 2. \ ∎ \tag{9}$$

Lemma 3. *We have*

$$S \equiv \begin{cases} \frac{am}{l}|G_{k'}| \bmod k'' & \textit{if } \mathrm{ord}_2\, l = \mathrm{ord}_2\, m \textit{ or } |G_{k'''}| \equiv 0 \bmod 2 \\ & \textit{or } a_j \equiv -1 \bmod 2^\nu \textit{ for some } j, \\ \frac{am}{l}|G_{k'}| + \frac{m}{2} \bmod k'' & \textit{otherwise.} \end{cases}$$

Proof. According to the definition of l and by the Lemma of [2] the quotient group $G/G_{k'}$ is isomorphic to the multiplicative group of residue classes mod k'' congruent to 1 mod l' and we have

$$G/G_{k'} = \{(ul'+1)G_{k'} : u = 0, 1, \ldots, k''/l' - 1\}.$$

Hence

$$\begin{aligned} S &\equiv |G_{k'}| \sum_{u=0}^{k''/l'-1} (ul'+1) \\ &= \frac{k''}{l'}|G_{k'}| + A \bmod k'' \quad \text{with} \quad A = \frac{k''/l'-1}{2}|G_{k'}|k''. \end{aligned}$$

It is easy to see that $k''/l' \equiv am/l \bmod k''$. We have $G_{k'''} \subseteq G_{k'}$. Hence if $\mathrm{ord}_2\, l = \mathrm{ord}_2\, m$ or $|G_{k'''}| \equiv 0 \bmod 2$ then $A \equiv 0 \bmod k''$. Assume that $a_j \equiv -1 \bmod 2^\nu$ for some j and $\mathrm{ord}_2\, l \neq \mathrm{ord}_2\, m$. By the definition of l, $l \equiv 2 \bmod 4$ and $m \equiv 0 \bmod 4$. By Lemma 2, $A \equiv 0 \bmod k''$.

Now assume that $\mathrm{ord}_2\, l \neq \mathrm{ord}_2\, m$ and $|G_{k'''}| \equiv 1 \bmod 2$ and $a_j \not\equiv -1 \bmod 2^\nu$ for each j. If $l \equiv 2 \bmod 4$ and $m \equiv 0 \bmod 4$ then by Lemma 2, $A \equiv 0 \equiv m/2 \bmod k''$. If $l \not\equiv 2 \bmod 4$ or $m \not\equiv 0 \bmod 4$ then $G_{k'} = G_{k'''}$ and $A \equiv k''/2 \equiv m/2 \bmod k''$. ∎

Lemma 4. *We have*

$$S \equiv \begin{cases} \frac{am}{l}|G_{k'}| \bmod 2^\kappa & \textit{if } \mathrm{ord}_2\, l = \mathrm{ord}_2\, m \textit{ or } |G_{k'''}| \equiv 0 \bmod 2 \\ & \textit{or } a_j \equiv -1 \bmod 2^\nu \textit{ for some } j, \\ \frac{am}{l}|G_{k'}| + \frac{m}{2} \bmod 2^\kappa & \textit{otherwise.} \end{cases}$$

Proof. If $l \not\equiv 2 \bmod 4$ or $m \not\equiv 0 \bmod 4$ then $\kappa = 0$ and the lemma holds trivially. So we may assume that $l \equiv 2 \bmod 4$ and $m \equiv 0 \bmod 4$. Then $\kappa = \nu \geq 2$. By Lemma 2, $\frac{m}{l}|G_{k'}| \equiv 0 \bmod 2^\nu$. Since $m/2 \equiv 2^{\nu-1} \bmod 2^\nu$ it is enough to prove that

$$S \equiv \begin{cases} 0 \bmod 2^\nu & \text{if } a_j \equiv -1 \bmod 2^\nu \text{ for some } j, \\ |G_{k'''}|2^{\nu-1} \bmod 2^\nu & \text{otherwise.} \end{cases}$$

Put $H = G_{k''k'''}$.

Assume that $a_j \equiv -1 \bmod 2^\nu$ for some j. We have $G/H = \{x_iH, -x_iH : i = 1, \ldots, s = [G:H]/2\}$, $x_i \equiv 1 \bmod 4$. Hence

$$S \equiv |H|\Big(\sum_{i=1}^{s} x_i - \sum_{i=1}^{s} x_i\Big) = 0 \bmod 2^\nu.$$

Assume now that $a_j \not\equiv -1 \bmod 2^\nu$ for each j. Since $l \equiv 2 \bmod 4$ and $m \equiv 0 \bmod 4$, we have $a_i \equiv -1 \bmod 4$ for some i. There exists a maximal ν_1 such that $2 \le \nu_1 \le \nu$ and

$$G/H = \{(u2^{\nu_1}+1)H, \varepsilon(u2^{\nu_1}+1)H : u = 0,1,\ldots,2^{\nu-\nu_1}-1\} \tag{10}$$

where $\varepsilon^2 \equiv 1 \bmod 2^{\nu_1}$, $\varepsilon \equiv -1 \bmod 4$.

We have $\nu_1 \ge 3$. Otherwise we would have $[G : H] = 2^{\nu-1}$ and $a_j \equiv -1 \bmod 2^\nu$ for some j, contrary to the assumption. We have four possibilities for ε: $\varepsilon \equiv 1 \bmod 2^{\nu_1}$, $\varepsilon \equiv 2^{\nu_1-1}+1 \bmod 2^{\nu_1}$, $\varepsilon \equiv 2^{\nu_1-1}-1 \bmod 2^{\nu_1}$, $\varepsilon \equiv -1 \bmod 2^{\nu_1}$. The first two possibilities are excluded since $\nu_1 \ge 3$ and $\varepsilon \equiv -1 \bmod 4$. Assume that $\varepsilon \equiv -1 \bmod 2^{\nu_1}$. By (10),

$$G/H = \{(u2^{\nu_1}+1)H, -(u2^{\nu_1}+1)H : u = 0,1,\ldots,2^{\nu-\nu_1}-1\}.$$

This means that $a_j \equiv -1 \bmod 2^\nu$ for some j, contrary to the assumption. Thus $\varepsilon \equiv 2^{\nu_1-1}-1 \bmod 2^{\nu_1}$. By (10) and Lemma 2,

$$\begin{aligned} S &\equiv |H|(1+\varepsilon)\sum_{u=0}^{2^{\nu-\nu_1}-1}(u2^{\nu_1}+1) \\ &= |H|(1+\varepsilon)2^{\nu-\nu_1} + |H|\frac{1+\varepsilon}{2}(2^{\nu-\nu_1}-1)2^\nu \\ &\equiv |H|(1+\varepsilon)2^{\nu-\nu_1} \equiv |H|2^{\nu-1} \equiv |G_{k'''}|2^{\nu-1} \bmod 2^\nu. \ \blacksquare \end{aligned}$$

LEMMA 5. *We have*

$$S \equiv \begin{cases} \frac{am}{l}|G_{k'}| \bmod m & \text{if } \operatorname{ord}_2 l = \operatorname{ord}_2 m \text{ or } |G_{k'''}| \equiv 0 \bmod 2 \\ & \text{or } a_j \equiv -1 \bmod 2^\nu \text{ for some } j, \\ \frac{am}{l}|G_{k'}| + \frac{m}{2} \bmod m & \text{otherwise.} \end{cases}$$

P r o o f. We have $m = 2^\kappa k''k'''$ and 2^κ, k'', k''' are pairwise relatively prime. Further, $m/l \equiv 0 \bmod k'''$ and $m/2 \equiv 0 \bmod k'''$ for $m \equiv 0 \bmod 2$. The lemma follows immediately from Lemmas 1, 3 and 4. ■

R e m a r k 1. Since $|G| = [G : G_{k'}]|G_{k'}| = \frac{k''}{l'}|G_{k'}|$, $\frac{m}{l}|G_{k'}|$ may be replaced by $k^{\mathrm{iv}}|G|$, where

$$k^{\mathrm{iv}} = \begin{cases} k' & \text{if } l \not\equiv 2 \bmod 4 \text{ or } m \not\equiv 0 \bmod 4, \\ k'/2 & \text{otherwise.} \end{cases}$$

PROPOSITION. $S \equiv 0 \bmod m$ *if and only if the following two conditions hold*:

(i) *either* $\operatorname{ord}_2 l = \operatorname{ord}_2 m$ *or* $|G_{k'''}| \equiv 0 \bmod 2$ *or* $a_j \equiv -1 \bmod 2^\nu$ *for some* j,

(ii) $|G_{k'}| \equiv 0 \bmod l$.

P r o o f. Sufficiency of (i) and (ii) follows immediately from Lemma 5. Assume that $S \equiv 0 \bmod m$. We shall show that (i) and (ii) are satisfied. If

(i) does not hold then $m \equiv 0 \bmod 4$ and we have

(11) $$l \equiv 0 \bmod 2, \quad a|G_{k'}| + l/2 \equiv 1 \bmod 2.$$

Indeed, if $l \equiv 0 \bmod 4$ then $\kappa = 0$, $a \equiv 1 \bmod 2$, $|G_{k'}| \equiv 1 \bmod 2$ and (11) follows. If $l \equiv 2 \bmod 4$ then (11) follows from Lemma 2. By Lemma 5, $a|G_{k'}| + l/2 \equiv 0 \bmod l$, contrary to (11). Thus (i) holds. By Lemma 5, $|G_{k'}| \equiv 0 \bmod l$. Thus (ii) holds. ■

3. Proof of Theorem 1. Let $\alpha \in O_k \setminus \{0\}$ and $\mathfrak{p}$ be a typical prime ideal of O_k prime to $m\alpha$. Since

$$\left(\frac{\alpha \,|\, K}{A}\right)_m = \left(\frac{\alpha \,|\, k_m}{A}\right)_m^{[K:k_m]}$$

for any ideal A of O_k prime to $m\alpha$ in virtue of the multiplicativity of the power residue symbol it is enough to prove that

(12) $$\left(\frac{\alpha \mid k_m}{\mathfrak{p}}\right)_m = \begin{cases} \left(\frac{\alpha|k}{\mathfrak{p}}\right)_n^{b[k_m:k_{m''}]} & \text{if } \operatorname{ord}_2 n = \operatorname{ord}_2 m \\ & \text{or } [k_m : k_{m''2^\mu}] \equiv 0 \bmod 2 \\ & \text{or the field } k \cap P_{2^\nu} \text{ is real,} \\ \left(\frac{\alpha|k}{\mathfrak{p}}\right)_n^{b[k_m:k_{m''}]+n/2} & \text{otherwise.} \end{cases}$$

Then (3) holds.

Put $G = \operatorname{Gal}(k_m/k) = \operatorname{Gal}(P_m/k \cap P_m)$. Then G can be viewed as a subgroup of the multiplicative group of residue classes mod m. We have the following decomposition in k_m:

(13) $$\mathfrak{p} = \prod_{i=1}^{g} P^{\sigma_{t_i}}$$

where $\sigma_{t_i}(\zeta_m) = \zeta_m^{t_i}$ for some t_i with $\bar{t}_i \in G$, and P is a prime ideal of O_{k_m}.

We have

(14) $$N_m P = (N\mathfrak{p})^f$$

where f is the degree of the ideal P with respect to the field k. Then f is also the smallest positive integer such that $(N\mathfrak{p})^f \equiv 1 \bmod m$. Further, $N_m P \equiv 1 \bmod m$ and $N\mathfrak{p} \equiv 1 \bmod n$.

Put $a_{ij} = t_i(N\mathfrak{p})^j$ ($i = 1, \ldots, g$; $j = 0, 1, \ldots, f-1$). It is known that $G = \{\bar{a}_{ij}\}_{i,j}$. Let l, S, l', k', k'', k''', κ, a be as in Lemma 1. We have

(15) $$S = \sum_{i,j} a_{ij} = \sum_{i=1}^{g}\sum_{j=0}^{f-1} t_i(N\mathfrak{p})^j = \frac{(N\mathfrak{p})^f - 1}{N\mathfrak{p} - 1}\sum_{i=1}^{g} t_i.$$

Further, $l = (\{a_{ij} - 1\}_{i,j}, m)$. By Galois theory, $l = n$. Hence

(16) $$l' = n', \quad k' = m', \quad k'' = m'', \quad k''' = m''', \quad \kappa = \mu, \quad a \equiv b \bmod n.$$

By Lemma 5, $Sn/m \in \mathbb{Z}$ and

$$(17)\quad S\frac{n}{m} \equiv \begin{cases} b|G_{m'}| \bmod n & \text{if } \operatorname{ord}_2 n = \operatorname{ord}_2 m \\ & \text{or } |G_{m'''}| \equiv 0 \bmod 2 \\ & \text{or } a_{ij} \equiv -1 \bmod 2^\nu \text{ for some } i \text{ and } j, \\ b|G_{m'}| + \frac{n}{2} \bmod n & \text{otherwise.} \end{cases}$$

By (13)–(15) and Euler's criterion,

$$\begin{aligned} \left(\frac{\alpha \mid k_m}{\mathfrak{p}}\right)_m &= \prod_{i=1}^{g} \left(\frac{\alpha \mid k_m}{P^{\sigma_{t_i}}}\right)_m = \prod_{i=1}^{g} \left(\frac{\alpha \mid k_m}{P}\right)_m^{\sigma_{t_i}} = \prod_{i=1}^{g} \left(\frac{\alpha \mid k_m}{P}\right)_m^{t_i} \\ &= \left(\frac{\alpha \mid k_m}{P}\right)_m^{\Sigma_{i=1}^g t_i} \equiv \alpha^{\frac{(N\mathfrak{p})^f-1}{m}\Sigma_{i=1}^g t_i} \\ &= \alpha^{\frac{N\mathfrak{p}-1}{n} S\frac{n}{m}} \equiv \left(\frac{\alpha \mid k_m}{\mathfrak{p}}\right)_n^{S\frac{n}{m}} \bmod P. \end{aligned}$$

Since P is prime to m, we obtain

$$(18)\qquad \left(\frac{\alpha \mid k_m}{\mathfrak{p}}\right)_m = \left(\frac{\alpha \mid k}{\mathfrak{p}}\right)_n^{S\frac{n}{m}}.$$

By Galois theory, $|G_{m'}| = [k_m : k_{m''}]$, $|G_{m'''}| = [k_m : k_{m''2^\mu}]$, the field $k \cap P_{2^\nu}$ is real if and only if the group G contains a residue class $\bmod\, m$ congruent to $-1 \bmod 2^\nu$. Now (12) follows immediately from (18) and (17). ∎

4. Proof of Theorem 2. If conditions (i) and (ii) are satisfied then (4) holds by Theorem 1. Assume that (4) holds. Let $\mathfrak{p}$ be a prime ideal of O_k prime to m and α be a number in O_k such that

$$(19)\qquad \left(\frac{\alpha \mid k}{\mathfrak{p}}\right)_n = \zeta_n.$$

We shall show that conditions (i) and (ii) are satisfied. If (i) is not satisfied then $m \equiv 0 \bmod 4$ and

$$(20)\qquad n \equiv 0 \bmod 2, \quad b[K : k_{m''}] + n/2 \equiv 1 \bmod 2.$$

Indeed, if $n \equiv 0 \bmod 4$ then $\mu = 0$, $b \equiv 1 \bmod 2$, $[K : k_{m''}] \equiv 1 \bmod 2$ and (20) follows. If $n \equiv 2 \bmod 4$ then by Lemma 2 and (16), $[K : k_{m''}] = [K : k_m]|G_{m'}| \equiv 0 \bmod 2$ and (20) follows again.

By Theorem 1 with $A = \mathfrak{p}$, (19) and (20) we have $\left(\frac{\alpha|K}{\mathfrak{p}}\right)_m \neq 1$, contrary to the assumption. Thus (i) holds. By (4) for $A = \mathfrak{p}$, Theorem 1 and (19) we obtain (ii). ∎

5. Proof of Corollary. Put $k = \mathbb{Q}$ in Theorem 2. The condition (i) is satisfied. Assume that $m \neq 2$ or the field K is of an even degree. By

Theorem 2 it is enough to prove that (ii) is satisfied. If $m \equiv 1 \bmod 2$ then $n = 1$ and obviously (ii) holds. If $m \equiv 0 \bmod 2$ then $n = 2$; $m'' = 2$ if $m \equiv 2 \bmod 4$, $m'' = 1$ if $m \equiv 0 \bmod 4$. Hence $k_{m''} = \mathbb{Q}$. If $m > 2$ then $[K : \mathbb{Q}] = [K : P_m][P_m : \mathbb{Q}] = [K : P_m]\varphi(m) \equiv 0 \bmod 2$. Thus (ii) holds. If $m = 2$ then $[K : \mathbb{Q}] \equiv 0 \bmod 2$. Thus (ii) holds again. ∎

Remark 2. The Corollary may be proved without using Theorem 2. For this purpose it is enough to use the equality $\sum_{i=1}^{\varphi(m)} r_i = \frac{1}{2} m\varphi(m)$, where $r_1, \ldots, r_{\varphi(m)}$ are all residues mod m prime to m contained between 0 and m.

References

[1] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper. Teil II: Reziprozitätsgesetz*, Würzburg–Wien, 1965.

[2] J. Wójcik, *Powers of cyclotomic numbers*, Comment. Math. 32 (1992), 213–223.

Received on 20.11.1992
and in revised form on 21.5.1993 (2339)