By definition $\mathrm{Tr}_{K/K_1}(|\beta|^2) = 0$. Thus we have $\mathrm{Tr}_{K\bar{K}/Q}(|\beta|^2) = 0$, which completes the proof of Theorem 3.

Now we give an example showing that results like Theorem 1 and 2 are no longer true for polynomials $f(x) \in K\bar{K}[x]$.

EXAMPLE. K is a totally complex field of fourth degree, the normal closure of which has a symmetric Galois group G.

By the Dirichlet Unit Theorem we have a unit α, $|\alpha| > 1$ with conjugates α, $\bar{\alpha}$, α_2, $\bar{\alpha}_2$. Then $|\alpha\alpha_2| = |\alpha\bar{\alpha}_2| = 1$. Replacing if necessary α by α^m, where m is a large positive integer, we can assume that

$$(1+|\alpha|^2)(1+|\alpha_2|^2) > 17.$$

We put $d = 1+|\alpha|^2$. We shall use the following notations:

$$d_{11'} = 1+|\alpha|^2, \quad d_{22'} = 1+|\alpha_2|^2, \quad d_{12} = 1+\alpha\alpha_2, \quad d_{1'2'} = 1+\bar{\alpha}\bar{\alpha}_2,$$
$$d_{1'2} = 1+\bar{\alpha}\alpha_2, \quad d_{12'} = 1+\alpha\bar{\alpha}_2.$$

Since G is symmetric all d_{ij} are conjugate.

Let γ be a nonzero element of K, m be a positive integer and let $\{\gamma, \bar{\gamma}, \gamma_2, \bar{\gamma}_2\}$ be the set of all conjugates of γ. Then we can write:

$$\begin{aligned} d_{11'}\mathrm{Tr}(d|\gamma|^{2m}) &= |d_{11'}\gamma^m + d_{1'2}\gamma_2^m + d_{1'2'}\bar{\gamma}_2^m|^2 + \\ &\quad + (d_{11'}d_{22'} - |d_{1'2}|^2 - |d_{12}|^2)|\gamma_2|^{2m} - d_{1'2}d_{12}\gamma_2^{2m} - d_{12'}d_{1'2'}\bar{\gamma}_2^{2m} \\ &= |d_{11'}\gamma^m + d_{1'2}\gamma_2^m + d_{1'2'}\bar{\gamma}_2^m|^2 + (d_{11'}d_{22'} - |d_{1'2}|^2 - \\ &\qquad - |d_{12}|^2)|\gamma_2|^{2m} + 2\mathrm{Re}(d_{1'2}d_{12}\gamma_2^m) \\ &\geqslant \big(d_{11'}d_{22'} - (|d_{12}| + |d_{1'2}|)^2\big)|\gamma_2|^{2m}. \end{aligned}$$

But $|d_{12}| = |1+\alpha\alpha_2| \leqslant 2$, $|d_{1'2}| = |1+\bar{\alpha}\alpha_2| \leqslant 2$ and $d_{11'}d_{22'} > 17$. Hence

$$\mathrm{Tr}(d|\gamma|^{2m}) \geqslant \frac{|\gamma_2|^{2m}}{1+|\alpha|^2} > 0.$$

References

[1] K. Győry, *Sur une classe des corps de nombres algebriques et ses applications*, Publ. Math. Debrecen 22 (1975), pp. 151–175.

[2] A. Schinzel, *Traces of polynomial in algebraic numbers*, K. Norske. Vidensk. Selsk. Skr. 6 (1975), pp. 1–3.

[3] G. Shimura and Y. Taniyama, *Complex multiplication of abelian varieties and its application to number theory*, Math. Soc. Japan 1961.

[4] N. Tschebotaröw und H. Schwerdtfeger, *Grundzüge der Galoisschen Theorie*, Groningen, Djakarta 1950.

Received on 17.11.1978
and in revised form on 10.6.1980 (1111)

ACTA ARITHMETICA
XLI (1982)

On the density of some sets of primes connected with cyclotomic polynomials

by

J. Wójcik (Warszawa)

I proved in [6] a certain result (Theorem 3 of [6]) about the so-called Lehmer numbers:

$$P_n' = P_n(\alpha, \beta) = \begin{cases} (\alpha^n-\beta^n)/(\alpha-\beta) & \text{if } n \text{ is odd,} \\ (\alpha^n-\beta^n)/(\alpha^2-\beta^2) & \text{if } n \text{ is even,} \end{cases}$$

where α, β are roots of the trinomial $z^2-\sqrt{L}z+M$ and L, M are rational integers.

The result in question is the following:

THEOREM. *If α, β are different from zero and α/β is not a root of unity, then there exists a positive integer k_0 such that for every positive integer k divisible by k_0 and for all positive integers D and r where $(D, r) = 1$ and $r \equiv 1 \bmod (D, k)$ there exist infinitely many primes q satisfying the conditions: $q \equiv r \bmod D$, $q \equiv 1 \bmod k$, $q \mid P_{(q-1)/k}(\alpha, \beta)$.*

The Dirichlet density of this set of primes is equal to $\dfrac{wT}{k\varphi([k, D])}$, where w, T are given in (24) of [6].

$[k, D]$ denotes the least common multiple of k and D.

The main aim of this paper is to generalize and to refine the above theorem. We shall also prove Theorem 2, connected with Schinzel's Conjecture H.

The afore said conjecture H reads as follows:

H. *If $f_1, f_2, \ldots, f_k$ are irreducible polynomials with integral coefficients and the leading coefficients positive such that $f_1(x) \ldots f_k(x)$ has no constant factor > 1 then there exist infinitely many positive integers x such that $f_1(x), \ldots, f_k(x)$ are primes.*

Definitions and notation. The terminology and notation are taken from [6]. $F_n(x)$ denotes the nth cyclotomic polynomial, $F_n(x, y) = y^{\varphi(n)}F_n(x/y)$.

Let us put

$$Q_n = Q_n(a, \beta) = \begin{cases} 1 & \text{if} \quad n = 1 \text{ or } 2, \\ F_n(a, \beta) & \text{if} \quad n \geqslant 3. \end{cases}$$

It is known that

$$P'_n = \prod_{d|n} Q_d \quad \text{and} \quad Q_n = \prod_{d|n} P_d'^{\mu(n/d)}.$$

We have

(1) $$Q_p = P'_p \quad \text{if } p \text{ is a prime.}$$

Q_n are *rational integers.*

Let us put

$$Q_{n,m} = Q_{n,m}(a, \beta) = \begin{cases} P'_m & \text{if} \quad n = 1, \\ F_n(a^m, \beta^m) & \text{if} \quad n \geqslant 2 \text{ and } (n, m) > 1, \\ F_n(a^m, \beta^m)/F_n(a, \beta) & \text{if} \quad n \geqslant 2 \text{ and } (n, m) = 1. \end{cases}$$

We have $Q_{n,1} = 1$, $Q_{2,m} = S_m$, where

$$S_m = S_m(a, \beta) = \begin{cases} (a^m+\beta^m)/(a+\beta) & \text{if} \quad m \text{ is odd,} \\ a^m+\beta^m & \text{if} \quad m \text{ is even.} \end{cases}$$

We have

(2) $$Q_{n,p} = Q_{np}, \quad \text{if} \quad n \text{ is a positive integer, } p \text{ a prime.}$$

Indeed, $Q_{1,p} = P'_p = Q_p$ by (1). If $n \geqslant 2$ then by the property of the cyclotomic polynomial $Q_{n,p} = F_{np}(a, \beta) = Q_{np}$ since $np \geqslant 3$.

We shall prove the following formulas:

(3) $$Q_{n,m} = \prod_{d|m_2} Q_{nm_1d} \quad \text{for} \quad (n, m) > 1,\ m = m_1m_2,\ (m_2, n) = 1,$$

where m_1 contains only prime factors dividing n;

(4) $$Q_{n,m} = \prod_{\substack{d|m \\ d>1}} Q_{nd} \quad \text{for} \quad (n, m) = 1.$$

Since Q_n are rational integers, it follows from these formulas that $Q_{n,m}$ are also *rational integers.*

We have

(5) $$F_n(x^m) = \prod_{d|m} F_{nd}(x) \quad \text{for} \quad (m, n) = 1.$$

Hence

(6) $$F_n(x^m) = F_{nm_1}(x^{m_2}) = \prod_{d|m_2} F_{nm_1d}(x),$$

where $m = m_1m_2$, $(m_2, n) = 1$, m_1 contains only prime factors dividing n. Hence $(nm_1, m_2) = 1$ and if, additionally, $(n, m) > 1$ then $m_1 > 1$, $n \geqslant 2$, $nm_1d \geqslant 3$ and by (6)

$$Q_{n,m} = F_n(a^m, \beta^m) = \prod_{d|m_2} F_{nm_1d}(a, \beta) = \prod_{d|m_2} Q_{nm_1d}.$$

Thus (3).

If $n \geqslant 2$, $(n, m) = 1$ and $d > 1$ then $nd \geqslant 3$ and by (5)

$$Q_{n,m} = F_m(a^m, \beta^m)/F_n(a, \beta) = \prod_{\substack{d|m \\ d>1}} F_{nd}(a, \beta) = \prod_{\substack{d|m \\ d>1}} Q_{nd}.$$

Thus (4) for $n \geqslant 2$. We have $Q_{1,m} = P'_m = \prod_{d|m} Q_d = \prod_{\substack{d|m \\ d>1}} Q_d$. Thus (4) for $n = 1$.

An algebraic integer is called *primitive* if it is not divisible by any positive integer > 1. We say that algebraic integers $a_1, \ldots, a_n$ are ***Z*-coprime** if there exists no positive integer $d > 1$ such that $d | a_1, \ldots, d | a_n$.

Let us put $k_1 = \boldsymbol{Q}(\sqrt{KL})$, where $K = L-4M$.

$$0 < d = (L, M) \quad \text{for} \quad \langle L, M\rangle \neq \langle 0, 0\rangle.$$

$$L_1 = \begin{cases} 0 & \text{if} \quad L = M = 0, \\ L/d & \text{if} \quad \langle L, M\rangle \neq \langle 0, 0\rangle; \end{cases} \qquad M_1 = \begin{cases} 0 & \text{if} \quad L = M = 0, \\ M/d & \text{if} \quad \langle L, M\rangle \neq \langle 0, 0\rangle; \end{cases}$$

$$a_1 = \begin{cases} 0 & \text{if} \quad L = M = 0, \\ a^2/d & \text{if} \quad \langle L, M\rangle \neq \langle 0, 0\rangle; \end{cases} \qquad \beta_1 = \begin{cases} 0 & \text{if} \quad L = M = 0, \\ \beta^2/d & \text{if} \quad \langle L, M\rangle \neq \langle 0, 0\rangle; \end{cases}$$

$K_1 = L_1 - 4M_1$.

We have $k_1 = \boldsymbol{Q}(\sqrt{K_1L_1})$. a_1, β_1 are roots of the trinomial $z^2-(L_1-2M_1)z+M_1^2$ with discriminant K_1L_1. Hence a_1, β_1 are *integers of* k_1; β_1 is the *conjugate of* a_1 if k_1 is quadratic.

Assume that a, β are different from zero and a/β is not a root of unity. We have $a/\beta = a_1/M_1 \in k_1$. Since $c_{k_1}(a/\beta)$ is a positive integer (Lemma 1 of [6]), there exists a maximal positive integer T such that

(7) $$a/\beta = \zeta_w^t \Xi^T,$$

where $\Xi = \gamma/\delta$, γ, δ are integers of k_1, γ, δ are $\boldsymbol{Z}$-coprime, δ is the conjugate of γ if k_1 is quadratic and w denotes the number of roots of unity in k_1.

We shall show that there exists a positive integer e such that

(8) $$M_1 = \pm e^T.$$

First we notice that $(L_1, M_1) = 1$ and $a_1+\beta_1 = L_1 - 2M_1$, $a_1\beta_1 = M_1^2$. Hence $(a_1, \beta_1) = 1$.

1. $k_1 = \boldsymbol{Q}$. We have $\Xi = \gamma/\delta$, $\gamma, \delta \in \boldsymbol{Z}$; $(\gamma, \delta) = 1$. $a/\beta = (-1)^t\gamma^T/\delta^T$; $a^2/\beta^2 = a_1/\beta_1 = \gamma^{2T}/\delta^{2T}$; $a_1, \beta_1 \in \boldsymbol{Z}$, $(a_1, \beta_1) = 1$. Hence $a_1 = \gamma^{2T}$, $\beta_1 = \delta^{2T}$

or $\alpha_1 = -\gamma^{2T}$, $\beta_1 = -\delta^{2T}$. Put $e = |\gamma\delta|$, where e is a positive integer. We have $M_1^2 = \alpha_1\beta_1 = (\gamma\delta)^{2T} = e^{2T}$. Hence $M_1 = \pm e^T$. Thus (8).

2. k_1 is quadratic. Below a dash denotes a conjugate number or a conjugate ideal. We have $\Xi = \gamma/\gamma'$. By (7) γ is a primitive integer of k_1.

We have

(i) If α_2, α_3 are primitive integers of k_1 and $\alpha_2/\alpha_2' = \alpha_3/\alpha_3'$ then $\alpha_2 = \pm\alpha_3$.

Indeed, $(\alpha_2/\alpha_3)' = \alpha_2/\alpha_3 \in \boldsymbol{Q}$. Thus $s\alpha_2 = r\alpha_3$, r, $s \in \boldsymbol{Z}$, $(r, s) = 1$, $s > 0$. Hence $r \mid \alpha_2$, $s \mid \alpha_3$. Since α_2, α_3 are primitive, it follows that $s = 1$, $r = \pm 1$. Thus (i).

(ii) If α_2 is a primitive integer of k_1 and $\mathfrak{p} \mid \alpha_2$, $\mathfrak{p} \mid \alpha_2'$, where $\mathfrak{p}$ is a prime ideal of k_1, then $\mathfrak{p}$ is ramified and $\mathfrak{p} \,\|\, \alpha_2$.

This is clear.

Let us put

(9) $\quad \gamma^2 = s\gamma_1,\quad$ where s is a positive integer and γ_1 a primitive integer of k_1.

We have

$$(\gamma_1, \gamma_1') = 1. \tag{10}$$

Indeed, if $\mathfrak{p} \mid \gamma_1$, $\mathfrak{p} \mid \gamma_1'$, where $\mathfrak{p}$ is a prime ideal then by (9) $\mathfrak{p} \mid \gamma$, $\mathfrak{p} \mid \gamma'$ and by (ii) $p = \mathfrak{p}^2$, where p is a prime, $\mathfrak{p}^2 \,\|\, \gamma^2$, $\mathfrak{p} \,\|\, \gamma_1$, $p \mid s$, $\mathfrak{p}^3 \mid \gamma^2$, and we obtain a contradiction.

By (7) and (9)

$$\alpha^2/\beta^2 = \alpha_1/\beta_1 = \zeta_w^{2t}\gamma^{2T}/\gamma'^{2T} = \zeta_w^t\gamma_1^T/\zeta_w^{-t}\gamma_1'^T.$$

Since $\beta_1 = \alpha_1'$, it follows from (i) and (10) that

$$\alpha_1 = \zeta_w^t\gamma_1^T,\quad \beta_1 = \zeta_w^{-t}\gamma_1'^T \quad \text{or} \quad \alpha_1 = -\zeta_w^t\gamma_1^T,\ \beta_1 = -\zeta_w^{-t}\gamma_1'^T. \tag{11}$$

Hence by (9) $M_1^2 = \alpha_1\beta_1 = N(\gamma_1)^T = e^{2T}$, where $e = |N(\gamma)/s|$ is a positive integer. Hence $M_1 = \pm e^T$. Thus (8).

If n is a rational integer, then n^* denotes the product of different prime numbers dividing n, $k_w(e)$ denotes the wth power-free kernel of e, $k(e)$ denotes the square-free kernel of e.

We shall prove the following

THEOREM 1. *Let n be any positive integer. Assume that α, β are different from zero and α/β is not a root of unity. Let $k > 0$ be an arbitrary common multiple of the numbers nw^2T and $8k(KL)k_w^*(e)$. For any positive integers D and r, where $(D, r) = 1$ and $r \equiv 1 \bmod (D, k)$, there exist infinitely many primes q satisfying the conditions*

$$q \equiv r \bmod D,\qquad q \equiv 1 \bmod k,\qquad q \mid Q_{n,(q-1)/k}.$$

The Dirichlet density of this set of primes is equal to $\dfrac{\varphi(n)wT}{k\varphi([k, D])}$, where e, w, T are given by (7) and (8).

THEOREM 2. *Let n be any positive integer. Assume that α, β are different from zero and α/β is not a root of unity. Then conjecture H implies the existence of infinitely many primes p such that Q_{np} is composite.*

Taking in Theorem 1 $n = 1$, we obtain

THEOREM 1′. *Assume that α, β are different from zero and α/β is not a root of unity. Let $k > 0$ be an arbitrary common multiple of the numbers w^2T and $8k(KL)k_w^*(e)$. For any positive integers D and r, where $(D, r) = 1$ and $r \equiv 1 \bmod (D, k)$, there exist infinitely many primes q satisfying the conditions*

$$q \equiv r \bmod D,\qquad q \equiv 1 \bmod k,\qquad q \mid P'_{(q-1)/k}.$$

The Dirichlet density of this set of primes is equal to $\dfrac{wT}{k\varphi([k, D])}$, where e, w, T are given by (7) and (8).

Taking $k_0 = [w^2T, 8k(KL)k_w^*(e)]$, we obtain Theorem 3 of [6].

Taking in Theorem 2 $n = 1$, we obtain by (1) Theorem 2 of [5].

LEMMA 1. *Let n, k be positive integers such that $n \mid k$, and $\alpha/\beta \in P_k$. Let $q \equiv 1 \bmod k$, $\mathfrak{q} \mid q$, where q is a prime and $\mathfrak{q}$ a prime ideal of P_k. Assume that q is prime to $KLMF_n(\alpha, \beta)$. Then $\left(\dfrac{\alpha/\beta}{\mathfrak{q}}\right)_k = \zeta_n^x$ for a certain $x \in \boldsymbol{Z}$, $(x, n) = 1$ if and only if $q \mid Q_{n,(q-1)/k}$.*

Proof. Necessity. $\mathfrak{q}$ is a prime ideal of degree one in P_k. Let $\left(\dfrac{\alpha/\beta}{\mathfrak{q}}\right)_k = \zeta_n^x$ for a certain x satisfying $(x, n) = 1$. Hence

$$F_n(\zeta_n^x) = 0. \tag{12}$$

We have

$$Q_{n,m} = F_n(\alpha^m, \beta^m)/A,\quad m \text{ being a positive integer,} \tag{13}$$

where

$$A = \begin{cases} \alpha^2-\beta^2 & \text{if} \quad n = 1,\ m \text{ is even,}\\ F_n(\alpha, \beta) & \text{if} \quad n \geqslant 2,\ (n, m) = 1 \text{ or } n = 1,\ m \text{ is odd,}\\ 1 & \text{if} \quad (n, m) > 1.\end{cases}$$

By Euler's criterion $(\alpha/\beta)^{(q-1)/k} \equiv \zeta_n^x \bmod \mathfrak{q}$ $\quad ((q, \alpha/\beta) = 1, (q, k) = 1)$. Hence by (12)

$$F_n(\alpha^{(q-1)/k}, \beta^{(q-1)/k}) = \beta^{\varphi(n)(q-1)/k}F_n\big((\alpha/\beta)^{(q-1)/k}\big) \equiv \beta^{\varphi(n)(q-1)/k}F_n(\zeta_n^x) \equiv 0 \bmod \mathfrak{q}.$$

Hence and by (13) $q \mid Q_{n,(q-1)/k}$ since $(q, A) = 1$.

Sufficiency. Assume that $q|Q_{n,(q-1)/k}$. Hence by (13)

$$\mathfrak{q} \mid \beta^{\varphi(n)(q-1)/k} F_n\big((\alpha/\beta)^{(q-1)/k}\big).$$

Since $(q, \beta) = 1$, it follows that

$$F_n\big((\alpha/\beta)^{(q-1)/k}\big) \equiv 0 \bmod \mathfrak{q}.$$

Thus

$$\prod_{(x,n)=1} [(\alpha/\beta)^{(q-1)/k} - \zeta_n^x] \equiv 0 \bmod \mathfrak{q}.$$

Since $\zeta_n \in P_k$, as $n|k$, the factors of the product belong to P_k. Hence $(\alpha/\beta)^{(q-1)/k} \equiv \zeta_n^x \bmod \mathfrak{q}$ for a certain x prime to n. By Euler's criterion $\left(\frac{\alpha/\beta}{\mathfrak{q}}\right)_k = \zeta_n^x$. The lemma is proved.

Proof of Theorem 1. Let $\Xi, \gamma, \delta, w, t, T$ have the meaning as in (7). We have $\delta = \gamma'$ if k_1 is quadratic. According to the definition of e we have $\gamma\delta = \pm se$, where $s = 1$ if $k_1 = Q$ and s is a positive integer satisfying (9) if k_1 is quadratic. Now we shall study s and e in the case of a quadratic k_1. Since γ is primitive, s is square-free by (9). If $p|s$, $\mathfrak{p}|p$, where $\mathfrak{p}$ is a prime ideal of k_1 and p is a prime, then by (9) $\mathfrak{p}|\gamma$, $\mathfrak{p}|\gamma'$ and by (ii) $p = \mathfrak{p}^2$. Hence s divides the discriminant of k_1 and $s|2k(KL)$. Further we have $e^2 = N(\gamma^2)/s^2 = N(\gamma_1) = \gamma_1\gamma_1'$ by the definition of e. If $p|e$, $\mathfrak{p}|p$, then $\mathfrak{p}' \neq \mathfrak{p}$ and $p = \mathfrak{p}\mathfrak{p}'$, and thus $(k(KL)|p) = 1$. Otherwise we would have $\mathfrak{p}' = \mathfrak{p}$, $\mathfrak{p}|\gamma_1$, $\mathfrak{p}|\gamma_1'$, contrary to (10). We have proved:

(iii) $\gamma\delta = \pm se$, where s is a square-free positive integer, s divides the discriminant of k_1, $s|2k(KL)$, e is a positive integer; if $p|e$ then $(k(KL)|p) = 1$, $(s, e) = 1$.

We shall use the theory of Gaussian sums. Let $k > 0$ be an arbitrary common multiple of the numbers nw^2T and $8k(KL)k_w^*(e)$.

Let us put $\mu = \alpha/\beta$. We have

(14) $$k_1 = Q(\sqrt{KL}) \subset P_{4|k(KL)|} \subset P_k, \quad \zeta_{w^2T} \in P_k.$$

We shall show that

(15) $$\mu = \nu^{wT}, \quad \nu \in P_k.$$

It is enough to prove that

(16) $$\Xi = \varkappa^w, \quad \varkappa \in P_k.$$

Then (15) is satisfied by $\nu = \zeta_{w^2T}^t \varkappa$ by (7) and (16).

1. $w = 2$. We have

(17) $$\Xi = \gamma/\delta = \gamma\delta/\delta^2 = (\sqrt{\pm se}/\delta)^2$$

by (iii). We have $k_w^*(e) = k(e)$. By (iii): $(s, e) = 1$, $k(se) = sk(e)$, $s|2k(KL)$, $\sqrt{\pm se} \in P_{4sk(e)} \subset P_{8|k(KL)|k_w^*(e)} \subset P_k$, $\delta \in k_1 \subset P_k$ by (14). By (17) $\varkappa = \sqrt{\pm se}/\delta$ satisfies (16).

2. $w = 4$. We have $k_1 = P_4 = Q(\sqrt{-1})$. We shall use the arithmetic of P_4. We have

(18) $\Xi = \gamma/\delta$, where γ, δ are primitive integers of P_4, $\delta = \bar{\gamma}$.

An integer of P_4 is called *primary* if it is congruent to 1 mod $2+2i$. Let us put

(19) $$\gamma = i^v(1+i)^{t_1}\pi_1^{x_1}\dots\pi_l^{x_l}\gamma_2^4, \quad \delta = i^{-v}(1-i)^{t_1}\bar{\pi}_1^{x_1}\dots\bar{\pi}_l^{x_l}\bar{\gamma}_2^4,$$

$1 \leqslant x_j \leqslant 3$, $p_j = \pi_j\bar{\pi}_j$, where p_j is a prime, $p_j \equiv 1 \bmod 4$, $\pi_j, \bar{\pi}_j$ are primary prime numbers of P_4, γ_2 is an integer of P_4, and t_1 equals 0 or 1.

Hence $\gamma\delta = 2^{t_1}p_1^{x_1}\dots p_l^{x_l}N(\gamma_2)^4$. On the other hand, by (iii), $\gamma\delta = N(\gamma) = se$, $s = 2^{t_1}$, $e = p_1^{x_1}\dots p_l^{x_l}N(\gamma_2)^4$,

(20) $$k_w^*(e) = k_4^*(e) = p_1\dots p_l.$$

By (18) and (19)

(21) $$\Xi = i^{2v+t_1}(\pi_1/\bar{\pi}_1)^{x_1}\dots(\pi_l/\bar{\pi}_l)^{x_l}(\gamma_2/\bar{\gamma}_2)^4.$$

Since one of the numbers $\bar{\pi}_j, -\bar{\pi}_j$ is primary in the sense of formula (11a) of [2], p. 443, we have by (10a) ibidem

(22) $$\tau^4(\bar{\chi}_j) = p_j\bar{\pi}_j^2 = p_j(-\bar{\pi}_j)^2, \quad \pi_j/\bar{\pi}_j = \big(\tau(\bar{\chi}_j)/\bar{\pi}_j\big)^4,$$

where

$$\tau(\bar{\chi}_j) = \sum_{x=1}^{p_j-1} \bar{\chi}_j(x)\zeta_{p_j}^x, \quad \chi_j(x) = \left(\frac{x}{\pi_j}\right)_4.$$

By (20)

$$\tau(\bar{\chi}_j) \in P_{4p_j} \subset P_{4p_1\dots p_l} = P_{4k_w^*(e)} \subset P_k, \quad \bar{\pi}_j \in P_4 \subset P_k.$$

Obviously $\zeta_{16} \in P_k$. By (21) and (22)

$$\varkappa = \zeta_{16}^{2v+t_1}\big(\tau(\bar{\chi}_1)/\bar{\pi}_1\big)^{x_1}\dots\big(\tau(\bar{\chi}_l)/\bar{\pi}_l\big)^{x_l}(\gamma_2/\bar{\gamma}_2)$$

satisfies (16).

3. $w = 6$. We have $k_1 = P_6 = P_3 = Q(\sqrt{-3})$. We shall use the arithmetic of P_3. We have

(23) $\Xi = \gamma/\delta$, where γ, δ are primitive integers of P_6, $\delta = \bar{\gamma}$.

An integer of P_6 is called *primary* if it is congruent to 1 mod 3.

Let us put

(24) $$\gamma = \zeta_6^v(1-\varrho^2)^{t_1}\pi_1^{x_1}\dots\pi_l^{x_l}\gamma_2^6, \quad \delta = \zeta_6^{-v}(1-\varrho)^{t_1}\bar{\pi}_1^{x_1}\dots\bar{\pi}_l^{x_l}\bar{\gamma}_2^6,$$

$\varrho = e^{2\pi i/3}$, $1 \leqslant x_j \leqslant 5$, $p_j = \pi_j \bar{\pi}_j$, where p_j is a prime, $p_j \equiv 1 \bmod 6$, π_j, $\bar{\pi}_j$ are primary prime numbers of P_6, γ_2 is an integer of P_6, t_1 equals 0 or 1. Hence

$$\gamma\delta = 3^{t_1} p_1^{x_1} \ldots p_l^{x_l} N(\gamma_2)^6.$$

On the other hand, by (iii),

$$\gamma\delta = N(\gamma) = se, \quad s = 3^{t_1}, \quad e = p_1^{x_1} \ldots p_l^{x_l} N(\gamma_2)^6,$$

$$k_w^*(e) = k_6^*(e) = p_1 \ldots p_l. \tag{25}$$

By (23) and (24)

$$\Xi = \zeta_6^{2v+t_1} (\pi_1/\bar{\pi}_1)^{x_1} \ldots (\pi_l/\bar{\pi}_l)^{x_l} (\gamma_2/\bar{\gamma}_2)^6. \tag{26}$$

Since $-\pi_j \equiv -1 \bmod 3$, we have by (10c) of [2], p. 445,

$$\tau^6(\chi_j\psi_j) = \hat{p}_j(-\bar{\pi}_j)^4 = \hat{p}_j \bar{\pi}_j^4, \quad \pi_j/\bar{\pi}_j = \left(\zeta_{12}^{(p_j-1)/2} \tau(\chi_j\psi_j)/\bar{\pi}_j\right)^6, \tag{27}$$

where

$$\hat{p}_j = (-1)^{(p_j-1)/2} p_j, \quad \tau(\chi_j\psi_j) = \sum_{x=1}^{p_j-1} \chi_j\psi_j(x) \zeta_{p_j}^x,$$

$$\psi_j(x) = \left(\frac{x}{p_j}\right), \quad \chi_j(x) = \left(\frac{x}{\pi_j}\right)_3.$$

By (25)

$$\tau(\chi_j\psi_j) \in P_{3p_j} \subset P_{3p_1\ldots p_l} = P_{3k_w^*(e)} \subset P_k, \quad \bar{\pi}_j \in P_3 \subset P_k.$$

Obviously ζ_{12}, $\zeta_{36} \in P_k$. By (26) and (27)

$$\varkappa = \zeta_{36}^{2v+t_1} \left(\zeta_{12}^{(p_1-1)/2} \tau(\chi_1\psi_1)/\bar{\pi}_1\right)^{x_1} \ldots \left(\zeta_{12}^{(p_l-1)/2} \tau(\chi_l\psi_l)/\bar{\pi}_l\right)^{x_l} (\gamma_2/\bar{\gamma}_2)$$

satisfies (16). (16) and hence also (15) are proved completely.

Let us put

$$\left(\frac{\theta}{\mathfrak{a}}\right)_s = \left(\frac{\theta \,|\, P_k}{\mathfrak{a}}\right)_s \quad \text{for } s \,|\, k, \quad m = k/wT. \tag{28}$$

By (15) μ, $\nu \in P_k$ and

$$\left(\frac{\mu}{\mathfrak{a}}\right)_k = \left(\frac{\nu}{\mathfrak{a}}\right)_m. \tag{29}$$

Let D be any positive integer. Let F be any positive integer divisible by $kDKLMF_n(\alpha, \beta)$ and by all conductors of power-residue symbols occurring in this proof. We have $P_k \subset P_F$.

Let us put

$$G_2 = \{s\colon s \in \boldsymbol{Q}, (s, F) = 1, s \equiv 1 \bmod k\}$$

(G_2 is a group of rationals mod F corresponding to the field P_k).

$$A = \{\mathfrak{a}\colon \mathfrak{a} \text{ an ideal of } P_k, (\mathfrak{a}, F) = 1\},$$

$$H_1 = \{\mathfrak{a}\colon \mathfrak{a} \text{ an ideal of } P_k, (\mathfrak{a}, F) = 1, N\mathfrak{a} \equiv 1 \bmod F\},$$

$$H = \left\{\mathfrak{a}\colon \mathfrak{a} \text{ an ideal of } P_k, (\mathfrak{a}, F) = 1, N\mathfrak{a} \equiv 1 \bmod F, \left(\frac{\mu}{\mathfrak{a}}\right)_k = 1\right\}.$$

By the assumption on F, A, H_1, H are groups of ideals mod F in virtue of Artin's reciprocity law.

Let $r \equiv 1 \bmod k$, $(r, F) = 1$, $r \in \boldsymbol{Q}$. Obviously $r \in G_2$. By Lemma 6 and (28) in [6] and by (7) and (15)

$$c_{\boldsymbol{Q}}(\mu) = wTc_{\boldsymbol{Q}}(\nu) = c_{\boldsymbol{Q}}(\Xi^T) = c_{\boldsymbol{Q}}(\Xi)\cdot T = wT.$$

Hence

$$c_{P_k}(\nu) = c_{\boldsymbol{Q}}(\nu) = 1. \tag{30}$$

According to the definition of k and by (28), $n \,|\, m$. By Lemma 4 of [6] for any x prime to n there exists an ideal $\mathfrak{a}_1^{(x)}$ of P_k such that

$$(\mathfrak{a}_1^{(x)}, F) = 1, \quad N\mathfrak{a}_1^{(x)} \equiv r \bmod F, \quad \left(\frac{\nu}{\mathfrak{a}_1^{(x)}}\right)_m = \zeta_n^x.$$

Let $C^{(x)}$ denote the coset of A with respect to H containing $\mathfrak{a}_1^{(x)}$, i.e. by (29)

$$C^{(x)} = \left\{\mathfrak{a}\colon \mathfrak{a} \text{ an ideal of } P_k, (\mathfrak{a}, F) = 1, N\mathfrak{a} \equiv r \bmod F, \left(\frac{\mu}{\mathfrak{a}}\right)_k = \zeta_n^x\right\}.$$

Put

$$h = (A : H). \tag{31}$$

Let $C = \bigcup_{\substack{x \bmod n \\ (x,n)=1}} C^{(x)}$ denote the set-theoretic union of the sets $C^{(x)}$.

Put

$$B = \{q\colon q \text{ a prime}, q \equiv r \bmod F, q \,|\, Q_{n,(q-1)/k}\}$$
$$(r \equiv 1 \bmod k, (r, F) = 1).$$

Let $\tau \in \mathrm{Gal}(P_k/\boldsymbol{Q})$. If $\mathfrak{q}$ is a prime ideal of P_k of degree one and $\mathfrak{q} \in C$ then $\tau\mathfrak{q} \in C$. Indeed, $q = N\mathfrak{q}$ is a prime number congruent to $1 \bmod k$, $\mathfrak{q} \,|\, q$, $\tau\mathfrak{q} \,|\, q$ and by Lemma 1 $q \in B$, $\tau\mathfrak{q} \in C$. Hence and by Lemma 1 if $\mathfrak{q}$ is a prime ideal of degree one in P_k and $\mathfrak{q} \in C$ then there exist exactly $|P_k|$ prime ideals of degree one in P_k, $\tau\mathfrak{q}$ ($\tau \in \mathrm{Gal}(P_k/\boldsymbol{Q})$) belonging to C and dividing a certain prime number q belonging to B ($q = Nq$). Conversely, if q is a prime number and $q \in B$ then q splits completely in P_k and each of its prime divisors belongs to C. Hence by Hecke's theorem and by (31)

$$d(C^{(x)}) = \frac{1}{h}, \quad d(C) = \sum_{\substack{x \bmod n \\ (x,n)=1}} d(C^{(x)}) = \frac{\varphi(n)}{h}, \tag{32}$$

$$d(C) = \lim_{s\to 1+0} \frac{\sum_{q\in C} 1/(Nq)^s}{\log\big(1/(s-1)\big)} = |P_k| \lim_{s\to 1+0} \frac{\sum_{q\in B} 1/q^s}{\log\big(1/(s-1)\big)} = |P_k| d(B).$$

Hence

$$d(B) = \varphi(n)/|P_k| h. \tag{33}$$

By Lemma 2 of [6] the quotient group A/H_1 is isomorphic to G_2/E_F. By the Galois theory

$$(A : H_1) = (G_2 : E_F) = (P_F : P_k) = |P_F|/|P_k|.$$

By Lemma 4 of [6] and by (29), (28), (30)

$$(H_1 : H) = m = k/wT.$$

By (31)

$$h = (A : H) = (A : H_1)(H_1 : H) = \frac{|P_F|}{|P_k|} \cdot \frac{k}{wT}.$$

By (33)

$$d(B) = \frac{\varphi(n) wT}{k\varphi(F)}. \tag{34}$$

Suppose that $D \equiv 0 \bmod k$. Put

$$B' = \{q\colon\ q \text{ a prime},\ q \equiv r \bmod D,\ q | Q_{n,(q-1)/k}\}$$

where $(r, D) = 1$ and $r \equiv 1 \bmod k$.

Let P be the group of all residue classes mod F prime to F and P_1 the subgroup of residue classes mod F congruent to 1 mod D. Since for each rational integer ξ prime to D there exists a rational integer η prime to F satisfying $\eta \equiv \xi \bmod D$, we have $(P : P_1) = \varphi(D)$. Hence the number of residue classes mod F which are congruent to r mod D is equal to $\varphi(F)/\varphi(D)$ and all the classes are congruent to 1 mod k because of $D \equiv 0 \bmod k$. It follows that the set B' apart from at most finite number of primes q dividing F is the set-theoretic union of $\varphi(F)/\varphi(D)$ disjoint sets of type B. Hence $d(B') = \big(\varphi(F)/\varphi(D)\big) d(B)$ and by (34)

$$d(B') = \varphi(n) wT/k\varphi(D). \tag{35}$$

Thus we have proved the theorem for $D \equiv 0 \bmod k$.

Let D be any positive integer. Let us put

$$B'' = \{q\colon\ q \text{ a prime number},\ q \equiv r \bmod D,\ q \equiv 1 \bmod k,\ q | Q_{n,(q-1)/k}\}$$

where $(r, D) = 1$ and $r \equiv 1 \bmod (D, k)$. There exist rational integers x, y such that $r = 1 + kx + Dy$. Obviously

$$B'' = \{q\colon\ q \text{ a prime number},\ q \equiv 1 + kx \bmod [k, D],\ q | Q_{n,(q-1)/k}\}.$$

By (35) (the theorem for $D \equiv 0 \bmod k$):

$$d(B'') = \varphi(n) wT/k\varphi([k, D]).$$

The theorem is proved.

LEMMA 2. *Let n be any positive integer. If α, β are different from zero and α/β is not a root of unity, then there exists a positive integer k divisible by $4nk(KL)$ and such that for every positive integer D there exist infinitely many primes q satisfying the condition*

$$q \equiv 1 \bmod k, \quad q | Q_{n,(q-1)/k}, \quad \big((q-1)/k, D\big) = 1.$$

Proof. Put $k = 8|k(KL)| k_w^*(e) n w^2 T$. Let D be any positive integer. $D = D_1 D_2$, where D_1 contains only prime factors dividing k and $(D_2, k) = 1$. Let r satisfy the system of congruences

$$r \equiv \begin{cases} k+1 \bmod k^2, \\ 2 \bmod D_2, \end{cases}$$

D_2 being odd since k is even. Hence $(r, Dk) = 1$, $r \equiv 1 \bmod k$. By Theorem 1 there exist infinitely many primes q satisfying the condition $q \equiv 1 \bmod k$, $q \equiv r \bmod Dk$, $q | Q_{n,(q-1)/k}$. Hence $\big((q-1)/k, D\big) = 1$. The lemma is proved.

Proof of Theorem 2. Let k be any positive integer satisfying Lemma 2. Put $N(\Omega) = N_{P_k/Q}(\Omega)$ and let for an abelian extension E/Ω, $f(E/\Omega)$ be its conductor. We have $Q(\alpha/\beta) = Q(\sqrt{KL})$. Hence $\alpha/\beta \in P_{4|k(KL)|} \subset P_k$. Let us put in Lemma 4 of [5] $k_2 = P_k$, $g(x) = F_k(x)$, $\theta = \zeta_k$,

$$F = k(2|P_k|)!\,|\mathrm{disc} F_k KLMQ_n|\, N\big(f(P_k(\sqrt[k]{\alpha/\beta})/P_k)\big).$$

By Lemma 2 there exists a prime q_0 such that

$$q_0 \equiv 1 \bmod k, \quad q_0 | Q_{n,(q_0-1)/k}, \quad \big((q_0-1)/k, F\big) = 1, \quad q_0 > F. \tag{36}$$

Since $q_0 \equiv 1 \bmod k$, q_0 splits in P_k. There exists a prime ideal $\mathfrak{a}$ in P_k such that

$$q_0 = N\mathfrak{a}. \tag{37}$$

By (36) and from the definition of F

$$F \equiv 0 \bmod k(2|P_k|)!\,\mathrm{disc} F_k, \quad N\mathfrak{a} \equiv 1 \bmod k, \quad (\mathfrak{a}, F) = 1,$$
$$\big((N\mathfrak{a} - 1)/k, F\big) = 1.$$

By Lemma 4 of [5] there exists a polynomial $f_1(x)$ such that the polynomials $f_1(x)$, $f_2(x) = (f_1(x)-1)/k$ satisfy the assumption of Conjecture H. By this conjecture there exist infinitely many positive integers x such that $q = f_1(x)$, $p = f_2(x)$ are primes. We may assume

$$q > |KLMQ_n|, \quad p > n. \tag{38}$$

Again by Lemma 4 in [5]

$$q = N\mathfrak{q}, \quad \mathfrak{q} \sim \mathfrak{a}^{-1} \bmod F, \tag{39}$$

where $\mathfrak{q}$ is a prime ideal of degree one in P_k.

By (36) and the definition of F: $q_0 > |KLMQ_n|$. By Lemma 1 and by (36) and (37)

$$\left(\frac{\alpha/\beta}{\mathfrak{a}}\right)_k = \zeta_n^x \quad \text{for a certain } x \text{ prime to } n.$$

Hence by Artin's reciprocity law and by (39)

$$\left(\frac{\alpha/\beta}{\mathfrak{q}}\right)_k = \left(\frac{\alpha/\beta}{\mathfrak{a}}\right)_k^{-1} = \zeta_n^{-x} \text{ for a certain } x \text{ prime to } n. \tag{40}$$

By (39) and (37) $q \equiv 1 \bmod k$. By (40), (39) and (38) and by Lemma 1 $q \,|\, Q_{n,(q-1)/k}$. Since $(q-1)/k = p$, we have

$$q \,|\, Q_{np} \tag{41}$$

by (2).

Without loss of generality we can assume that $L > 0$. Then for $K > 0$ we have in virtue of (4.1) of [4] and by (38)

$$|Q_{np}| > R^{\frac{1}{2}\varphi(n)(p-1)},$$

where

$$R = \begin{cases} |4LM| & \text{if} \quad M < 0, \\ |4KM| & \text{if} \quad M > 0 \end{cases}$$

and for $K < 0$ for $p > N(\alpha, \beta)/n$ by the fundamental lemma of [3]

$$|Q_{np}| > |\alpha|^{\varphi(n)(p-1)-2^{\nu(n)+1}\log^3 np} \geqslant \sqrt{2}^{\,\varphi(n)(p-1)-2^{\nu(n)+1}\log^3 np}, \tag{42}$$

where $\nu(n)$ denotes the number of prime factors of n.

Thus in any case for p large enough we have $|Q_{np}| > kp+1 = q$ and (41) implies that Q_{np} is composite. The assertion of Theorem 2 follows.

Remark. Using Baker's theorem [1], one can obtain an inequality stronger than (42), namely

$$|Q_{np}(\alpha, \beta)| \geqslant \sqrt{2}^{\,\varphi(n)(p-1)-c_1 2^{(\nu(n)+1)}\log np},$$

where $c_1 = c_1(\alpha, \beta)$, $p > n$ provided $L > 0$, $K < 0$, $M \neq 0$, and α/β is not a root of unity.

If α/β is a *non-trivial unit*, then we have

$$\alpha/\beta = \begin{cases} \pm\varepsilon_1^{\pm T} & \text{if} \quad N(\varepsilon_1) = 1, \\ \pm\varepsilon_1^{\pm 2T} & \text{if} \quad N(\varepsilon_1) = -1 \end{cases} \tag{43}$$

where ε_1 is the fundamental unit of k_1.

Hence

$$T = \begin{cases} \big|\log|\alpha/\beta|\big|/\log|\varepsilon_1| & \text{if} \quad N(\varepsilon_1) = 1, \\ \big|\log|\alpha/\beta|\big|/2\log(\varepsilon_1) & \text{if} \quad N(\varepsilon_1) = -1. \end{cases}$$

Put $T = \infty$ if $\alpha = 0$ or $\beta = 0$ or α/β is a root of unity. Below we shall study the computation of $T = T(L, M)$. We have

(i) α/β is unit if and only if $|M_1| = 1$, i.e. $M \,|\, L$.

Indeed, the trinomial $z^2-(L/M-2)z+1$ has roots α/β and β/α. α/β is a unit if and only if $M \,|\, L$, i.e. $|M_1| = 1$.

(ii) α or β is zero if and only if $M_1 = 0$.

This is clear.

Let us put

$$T_{\max} = \begin{cases} \text{maximal } T_1 \text{ satisfying: } M_1 = \pm e_1^{T_1},\ e_1 \text{ a positive integer} \\ \hfill \text{for } |M_1| > 1, \\ \infty \quad \text{for } |M_1| = 0 \text{ or } 1. \end{cases}$$

By (i) and (ii)

$$T_{\max} = \infty \quad \text{if and only if } \alpha = 0 \text{ or } \beta = 0 \text{ or } \alpha/\beta \text{ is a unit.} \tag{44}$$

Hence by (8)

$$T \leqslant T_{\max}. \tag{45}$$

PROPOSITION. *If $k_1 = \boldsymbol{Q}$ or k_1 is a quadratic imaginary field with class number 1 or 2, then $T = T_{\max}$.*

If $\alpha = 0$ or $\beta = 0$ or α/β is a root of unity, then by (44) $T = T_{\max} = \infty$. Assume that α, β are different from zero and α/β is not a root of unity. Then T, $T_{\max}$ are finite. We have $M_1 = \pm e_1^{T_{\max}}$, where e_1 is a positive integer. Hence

$$\alpha_1\beta_1 = M_1^2 = e_1^{2T_{\max}}. \tag{46}$$

$k_1 = \boldsymbol{Q}$. Since α_1, β_1 are rational integers and $(\alpha_1, \beta_1) = 1$, we have

$$\alpha_1 = \varepsilon\gamma^{2T_{\max}}, \quad \beta_1 = \varepsilon\delta^{2T_{\max}}, \quad \varepsilon^2 = 1, \quad \gamma, \delta \in \boldsymbol{Z}, \quad (\gamma, \delta) = 1.$$

Hence

$$\alpha^2/\beta^2 = \alpha_1/\beta_1 = (\gamma/\delta)^{2T_{\max}}, \quad \alpha/\beta = \pm(\gamma/\delta)^{T_{\max}}.$$

Hence, by the definition of T, $T_{\max} \leqslant T$. By (45) $T = T_{\max}$.

k_1 *is quadratic imaginary*. Since α_1, β_1 are integers of k_1, $(\alpha_1, \beta_1) = 1$, $\beta_1 = \alpha_1'$, by (46) there exists an integral ideal $\mathfrak{a}$ of k_1 such that

$$(\alpha_1) = \mathfrak{a}^{2T_{\max}}, \quad (\beta_1) = \mathfrak{a}'^{2T_{\max}}. \tag{47}$$

Since k_1 has the class number 1 or 2, we have $\mathfrak{a}^2 = (\gamma_1)$ where γ_1 is an integer of k_1.

Hence $N(\gamma_1/N\mathfrak{a}) = 1$. By Hilbert's Theorem 90 $\gamma_1/N\mathfrak{a} = \gamma/\gamma'$, where γ is a primitive integer of k_1. Hence $\mathfrak{a}/\mathfrak{a}' = (\gamma_1)/(N\mathfrak{a}) = (\gamma_1/N\mathfrak{a}) = (\gamma/\gamma')$ and by (47)

$$(\alpha/\beta)^2 = (\alpha^2/\beta^2) = (\alpha_1/\beta_1) = (\mathfrak{a}/\mathfrak{a}')^{2T_{\max}} = (\gamma/\gamma')^{2T_{\max}}.$$

Hence $(\alpha/\beta) = (\gamma/\gamma')^{T_{\max}}$. Passing to the numbers, we have $\alpha/\beta = \zeta_w^t(\gamma/\gamma')^{T_{\max}}$. Hence $T_{\max} \leqslant T$ and by (45) $T = T_{\max}$.

Now we shall give some method of finding $T = T(L, M)$. By (43) and by the proposition we may assume that α, β are different from zero and α/β is not a unit, and k_1 is a real quadratic field or an imaginary quadratic field with class number > 2. In particular $k_1 \neq P_3, P_4$. We have $T < \infty$, $T_{\max} < \infty$, $w = 2$. T may be defined as follows:

(iv) T = maximal T_1, satisfying the following condition: $T_1 | T_{\max}$, $\alpha_1 = \pm\gamma_2^{T_1}$, there exists a rational integer s_1 such that $s_1\gamma_2 = \gamma_3^2$, $\gamma_3 \in k_1$, s_1 divides the discriminant of k_1 and s_1 is squarefree.

Indeed, by (8), (9), (11) and (iii), $T | T_{\max}$, $\alpha_1 = \pm\gamma_1^T$, $s_1\gamma_1 = \gamma^2$, $\gamma_1, \gamma \in k_1$ and s_1 is squarefree and divides the discriminant of k_1. On the other hand, if $\alpha_1 = \varepsilon\gamma_2^{T_1}$, $\varepsilon^2 = 1$, $\gamma_2 \in k_1$, $s_1\gamma_2 = \gamma_3^2$, $\gamma_3 \in k_1$, $s_1 \in Q$, then $\beta_1 = \varepsilon\gamma_2'^{T_1}$, $s_1\gamma_2' = \gamma_3'^2$ and $\alpha^2/\beta^2 = \alpha_1/\beta_1 = (\gamma_2/\gamma_2')^{T_1} = (\gamma_3/\gamma_3')^{2T_1}$. Hence $\alpha/\beta = \pm(\gamma_3/\gamma_3')^{T_1}$. Thus $T_1 \leqslant T$.

Let us put

$$\omega = \begin{cases} \sqrt{k(KL)} & \text{if} \quad k(KL) \not\equiv 1 \bmod 4, \\ (1+\sqrt{k(KL)})/2 & \text{if} \quad k(KL) \equiv 1 \bmod 4. \end{cases}$$

The numbers $1, \omega$ form an integral basis of k_1. Since α_1 is an integer, γ_2, γ_2' are also integers.

By (iv) we shall find T if we solve a finite number of equations of the form $a + b\omega = (x+y\omega)^m = f(x,y) + g(x,y)\omega$ in rational integers x, y where $a, b \in \mathbf{Z}$, $b \neq 0$, and m is a positive integer. f, g are forms of degree m with rational integral coefficients. The above equation is equivalent to the system of equations

$$\begin{cases} f(x,y) = a, \\ g(x,y) = b, \quad a, b \in \mathbf{Z},\ b \neq 0. \end{cases} \tag{48}$$

This system may be solved by using the elimination theory. We shall use a certain method independent of elimination theory. For any rational integers x, y satisfying (48) we have $a + b\omega \equiv x^m \bmod y$.

Hence $b \equiv 0 \bmod y$. If x_0, y_0 satisfy (48), then $y_0 | b$, x_0 satisfies the equation $f(x, y_0) - a = x^m + A_1x^{m-1} + \ldots + A_m = 0$, where $A_1, \ldots, A_m$ are rational integers, $g(x_0, y_0) = b$. Conversely, every such x_0, y_0 satisfy (48). After a finite number of steps we shall find the solution x_0, y_0 of system (48) if there exists a solution.

EXAMPLE 1. $L = 6$, $M = 128$. We have $L_1 = 3$, $M_1 = 2^6$, $T_{\max} = 6$, $T|6$. α_1, β_1 are roots of the trinomial $z^2 + 125z + 4096$. $K = L - 4M = -506$. $k_1 = \mathbf{Q}(\sqrt{-759})$, $\omega = (1+\sqrt{-759})/2$, $\alpha_1 = -63+\omega$, $\beta_1 = -63+\omega'$. None of the equations $-63+\omega = \pm(x+y\omega)^2$, $-63+\omega = (x+y\omega)^3$ is soluble. We have $3(-63+\omega) = (1+\omega)^2$. Hence $T = 1$.

EXAMPLE 2. $L = 6$, $M = -128$. We have $L_1 = 3$, $M_1 = -2^6$, $T_{\max} = 6$, $T|6$. $K = 518$, $k_1 = \mathbf{Q}(\sqrt{777})$. α_1, β_1 are roots of the trinomial $z^2 - 131z + 4096$, $\omega = (1+\sqrt{777})/2$. $\alpha_1 = 65+\omega$, $\beta_1 = 65+\omega'$. None of the equations $65+\omega = \pm(x+y\omega)^2$, $65+\omega = (x+y\omega)^3$ is soluble. We have $3(65+\omega) = (1+\omega)^2$. Hence $T = 1$.

EXAMPLE 3. $L = 256$, $M = 36$. We have $L_1 = 64$, $M_1 = 3^2$, $T_{\max} = 2$, $T|2$. α_1, β_1 are roots of the trinomial $z^2 - 46z + 81$. $K = 112$. $k_1 = \mathbf{Q}(\sqrt{7})$, $\omega = \sqrt{7}$, $\alpha_1 = 23+8\sqrt{7}$, $\beta_1 = 23-8\sqrt{7}$. We have $23+8\sqrt{7} = (4+\sqrt{7})^2$, $2(4+\sqrt{7}) = (1+\sqrt{7})^2$. Hence $T = 2$.

References

[1] A. Baker, *A sharpening of the bounds for linear forms in logarithms*, Acta Arith. 21 (1972), pp. 117–129.

[2] H. Hasse, *Vorlesungen über Zahlentheorie*, Berlin, Göttingen, Heidelberg 1950.

[3] A. Schinzel, *The intrisic divisors of Lehmer numbers in the case of negative discriminant*, Arkiv för Mat. 4 (1962), pp. 413–416.

[4] M. Ward, *The intrinsic divisors of Lehmer numbers*, Ann. of Math. 62 (1955), pp. 230–236.

[5] J. Wójcik, *On the composite Lehmer numbers with prime indices III*, Colloq. Math. 45(1981), pp. 81–90.

[6] — *Contributions to the theory of Kummer extensions*, Acta Arith. 40 (1982), pp. 155–174.

Received on 7.9.1979
and in revised form on 14.4.1980 (1169)