COLLOQUIUM MATHEMATICUM

VOL. XXX 1974 FASC. 1

ON SEQUENCES OF ALGEBRAIC INTEGERS IN PURE EXTENSIONS OF PRIME DEGREE

BY

R. WASÉN (WARSZAWA)

In 1965, J. Browkin asked whether there exists an infinite sequence $a_1, a_2, \ldots, a_n, \ldots$ of integers in $Q(i)$ such that, for all ideals q of $Q(i)$, integers $a_1, a_2, \ldots, a_{N(q)}$ represent all residue classes modulo q. Clearly, the sequence of natural numbers is such a sequence in Q.

In 1966, E. G. Straus answered this question in the negative. In 1969, B. Wańtuła has proved in an unpublished M. A. dissertation that no such sequence exists in any quadratic field.

In 1969, A. Schinzel proposed the following problem at the Institute on Number Theory at Stony Brook 1968/69:

Let K be an algebraic number field. Does there exist a sequence $\{a_i\}$ of integers in K such that, for every ideal q of K, integers $a_1, a_2, \ldots, a_{N(q)}$ represent all residue classes modulo q?

In 1971, the author proved that there exists no such sequence in any pure cubic field. The same year D. Barsky proved that, for any algebraic number field of degree greater than one, no such sequence exists (see [1]).

Now the natural question arises whether, for a given algebraic number field K, there is a maximal length of sequences $\{a_i\}_1^m$ such that, for all ideals q, the $\min(m, N(q))$ first terms represent different residue classes modulo q? Clearly, $\langle 0, 1\rangle$ is such a sequence of length 2 in any algebraic number field. If such a maximal length exists for K, we call it $m(K)$, otherwise we say that $m(K) = \infty$.

In the above-mentioned papers it has been shown that $m(K) < \infty$ if K is a quadratic or a pure cubic field. In the paper of the author there is a proof due to A. Schinzel that $m(K) = 4$ if $K = Q(\sqrt[3]{2})$ and all sequences of maximal length are actually found.

I would like to thank Prof. Schinzel for many valuable suggestions and help in the preparation of this manuscript.

In 1971, Latham proved (see [4]) that $m(K) = 2$ for all cubic fields with negative discriminant with only finitely many possible exceptions. For pure cubic fields, he proved that $m(K) = 2$ if $K \neq Q(\sqrt[3]{2})$ and gave an independent proof of the above-mentioned result concerning $Q(\sqrt[3]{2})$. Latham also constructed infinite classes of cubic fields with positive discriminants such that $m(K) = 2$ and did the same for quartic fields.

THEOREM 1. *A sequence of distinct terms $\{a_i\}_1^{\mathfrak{m}}$ has the property that, for every initial segment $\{a_i\}_1^m$ and for every ideal q such that $N(q) \geqslant m$, $a_1, a_2, \ldots, a_m$ represent m different residue classes modulo q if and only if $|N(a_i - a_j)| < \max(i, j)$ for all $i, j \leqslant \mathfrak{m}$.*

Proof. Suppose that a sequence $\{a_i\}_1^{\mathfrak{m}}$ of distinct integers of K has the required property and that there exist $i, j \leqslant \mathfrak{m}$ such that $|N(a_i - a_j)| \geqslant \max(i, j)$. Consider the initial segment $\{a_i\}_1^{\max(i,j)}$ and the principal ideal $q = (a_i - a_j)$. By a well-known theorem (see [3], § 27, p. 28), $|N(a_i - a_j)| = N(q) \geqslant \max(i, j)$, and so $a_1, \ldots, a_{\max(i,j)}$ would represent $\max(i, j)$ different residue classes modulo $(a_i - a_j)$ which is absurd since $a_i \equiv a_j \pmod{(a_i - a_j)}$.

On the other hand, suppose that $|N(a_i - a_j)| < \max(i, j)$ for all $i, j \leqslant \mathfrak{m}$ and that there exist an initial segment $\{a_i\}_1^m$ and an ideal q such that $N(q) \geqslant m$, so that $a_1, \ldots, a_m$ represent at most $m - 1$ residue classes modulo q. Suppose that $a_i \equiv a_j \pmod{q}$, $i \neq j$; thus $q | (a_i - a_j)$ which implies that $|N(a_i - a_j)| = lN(q)$, $l \in N$. Since $a_i \neq a_j$ if $i \neq j$ and the norm of a number is zero if and only if the number is zero, we have, clearly, $l \neq 0$, and so $|N(a_i - a_j)| \geqslant N(q)$. Now $\max(i, j) > |N(a_i - a_j)|$ and so $\max(i, j) > N(q) \geqslant m$ which is, clearly, impossible since i and j are indices for two of the first m numbers.

Every sequence satisfying the equivalent conditions given in Theorem 1 will be called an *F-sequence of length* $\mathfrak{m}$. The problem of Schinzel is, clearly, equivalent to the problem of existence of an infinite F-sequence.

Definition 1. An F-sequence $\{a_i\}$ is *basal* if $a_1 = 0$ and $a_2 = 1$.

The following lemma gives sense to this definition:

LEMMA 1. *To every F-sequence of integers of K there corresponds in K a basal F-sequence of the same length.*

Proof. Consider an F-sequence $\{a_i\}_1^{\mathfrak{m}}$ and put $a_i' = a_i - a_1$. Then, clearly, $a_1' = 0$ and $\{a_i'\}_1^{\mathfrak{m}}$ is an F-sequence. By Theorem 1,

$$1 \geqslant |N(a_2' - a_1')| = |N(a_2' - 0)| = |N(a_2')|,$$

and thus $N(a_2') = \pm 1$ and $a_2'^{-1}$ is an integer of K. We set $a_i'' = a_i'(a_2')^{-1}$. Clearly, $\{a_i''\}_1^m$ is a basal F-sequence.

In the sequel, m^* will denote the product of all distinct primes dividing a rational integer m, p an odd prime, and ζ_p a p-th root of unity.

Definition 2. A pure extension $Q(\sqrt[p]{a})$ of prime-degree p *is of class* A if there exists a rational integer m such that $m = m_1^1 m_2^2 \dots m_{p-1}^{p-1}$, where m_i are positive squarefree and pairwise coprime rational integers, $Q(\sqrt[p]{a}) = Q(\sqrt[p]{m})$, and

$$(m_1^1 m_2^2 \dots m_{p-2}^{p-2})^{p-1} - m_{p-1}^{p-1} \not\equiv 0 \pmod{p^2}$$

and is of class B otherwise. $\sqrt[p]{m}$ will then be called a *reduced generator* of $Q(\sqrt[p]{a})$.

Clearly, m is a positive rational integer not divisible by the p-th power of any prime. Moreover, m can be written uniquely in the form $m = m_1^1 m_2^2 \dots m_{p-1}^{p-1}$, where m_i are positive squarefree pairwise coprime rational integers. This follows easily from the fundamental theorem of arithmetics. In the sequel, any such representation will be supposed to fulfill these conditions. Obviously, every pure extension has at least one reduced generator. In order to prove that the definition makes sense, i.e., that any pure extension of prime-degree belongs to one and only one of the classes A and B, it is enough to show that if $\sqrt[p]{m}$ and $\sqrt[p]{m'}$ are two reduced generators of $Q(\sqrt[p]{a})$ and

$$m = m_1^1 m_2^2 \dots m_{p-1}^{p-1}, \qquad m' = m_1'^1 m_2'^2 \dots m_{p-1}'^{p-1},$$

then

$$(m_1^1 m_2^2 \dots m_{p-2}^{p-2})^{p-1} \equiv m_{p-1}^{p-1} \pmod{p^2}$$

iff

$$(m_1'^1 m_2'^2 \dots m_{p-2}'^{p-2})^{p-1} \equiv m_{p-1}'^{p-1} \pmod{p^2}.$$

In order to establish this we need the following lemma:

Lemma 2. *Fields* $Q(\sqrt[p]{a})$ *and* $Q(\sqrt[p]{b})$ *are identical if and only if* $b = a^r c^p$, *where* $0 \leqslant r < p$, $a, b, c \in Q$, $\sqrt[p]{a}$ *and* $\sqrt[p]{b}$ *reals.*

Proof. The "if" part is trivial.

In order to prove the remainder, let us observe that, by a result of Siegel (see [5]), the degree of $Q(\sqrt[p]{a}, \sqrt[p]{b})$ over $Q(\sqrt[p]{a})$ is equal to the least positive integer d such that $(\sqrt[p]{b})^d = (\sqrt[p]{a})^r c$ for a suitable integer r and a suitable $c \in Q$. If $\sqrt[p]{b} \in Q(\sqrt[p]{a})$, we get at once $b = a^r c^p$, $0 \leqslant r < p$ and $c \in Q$.

Now suppose that $\sqrt[p]{m}$ and $\sqrt[p]{m'}$ are two reduced generators of $Q(\sqrt[p]{a}) \neq Q$. By Lemma 2, $f^p m' = m^r e^p$, where e and f are rational positive coprime integers and $0 < r < p$. It follows that $e = 1$. Now, if $m = m_1^1 m_2^2 \dots m_{p-1}^{p-1}$, we have

$$f^p m' = m_1^r m_2^{2r} \dots m_{p-1}^{(p-1)r} = m_1^{\bar{r}} m_2^{\overline{2r}} \dots m_{p-1}^{\overline{(p-1)r}} (m_1^{\lambda_1} m_2^{\lambda_2} \dots m_{p-1}^{\lambda_{p-1}})^p,$$

where $rj = \lambda_j p + \bar{rj}$, and $0 < \bar{rj} < p$. It follows that $m' = m_1^{\bar{r}} m_2^{\overline{2r}} \dots m_{p-1}^{\overline{(p-1)r}}$.

With the same argument it follows that if $m' = m_1'^1 m_2'^2 \dots m_{p-1}'^{p-1}$, there exists an s, $0 < s < p$, such that

$$m = m_1'^{\bar{s}} m_2^{\overline{2s}} \dots m_{p-1}^{\overline{(p-1)s}}, \qquad is = \lambda_i p + \overline{is}, \ 0 < \overline{si} < p.$$

Moreover, since $0 < r < p$, $\overline{ri} \neq \overline{rj}$ if $i \neq j$, $1 \leqslant i$, and $j \leqslant p-1$. Hence $m_i' = m_j$, where j is such that $rj \equiv i \pmod p$. Using the fact that there exists an r such that $0 < r < p$ and $m' = m_1^{\bar{r}} m_2^{\overline{2r}} \dots m_{p-1}^{\overline{(p-1)r}}$, we show that

$$(m_1^1 m_2^2 \dots m_{p-2}^{p-2})^{p-1} \equiv m_{p-1}^{p-1} \pmod{p^2}$$

implies

$$(m_1'^1 m_2'^2 \dots m_{p-2}'^{p-2})^{p-1} \equiv m_{p-1}'^{p-1} \pmod{p^2},$$

and this, in view of the symmetry between m and m', completes the proof that any pure extension of prime-degree belongs to one and only one of the classes A and B.

Suppose that

$$(m_1^1 m_2^2 \dots m_{p-2}^{p-2})^{p-1} \equiv m_{p-1}^{p-1} \pmod{p^2}.$$

By regrouping, we get

$$m_k^{k(p-1)} (m_1^1 \dots m_{k-1}^{k-1} \dots m_{k+1}^{k+1} \dots m_{p-2}^{p-2})^{p-1} \equiv m_{p-1}^{p-1} \pmod{p^2}.$$

Since we may suppose that $m_k \not\equiv 0 \pmod p$,

$$(m_1^1 \dots m_{k-1}^{k-1} m_{k+1}^{k+1} \dots m_{p-2}^{p-2})^{p-1} \equiv m_{p-1}^{p-1} m_k^{-k(p-1)} \pmod{p^2}.$$

Now, if $r = 1$, then $m = m'$ and the proof follows directly from the fact that, for any reduced generator $\sqrt[p]{m}$, m can be written uniquely in the form $m = m_1^1 m_2^2 \dots m_{p-1}^{p-1}$. So we may suppose that $1 < r < p$. Hence, there exists an l, $1 \leqslant l \leqslant p-2$, such that $lr \equiv p-1 \pmod p$. Moreover, if $i \equiv j \pmod p$, then

$$a^{i(p-1)} \equiv a^{j(p-1)} \pmod{p^2} \quad \text{for all } a.$$

Using these observations, we get, with $k = l$,

$$\begin{aligned}
(m_1'^1 m_2'^2 \dots m_{p-2}'^{p-2})^{p-1} &\equiv (m_1^r \dots m_{k-1}^{(k-1)r} m_{k+1}^{(k+1)r} \dots m_{p-2}^{(p-2)r} m_{p-1}^{(p-1)r})^{p-1} \\
&\equiv (m_1^1 \dots m_{k-1}^{k-1} m_{k+1}^{k+1} \dots m_{p-2}^{p-2})^{r(p-1)} m_{p-1}^{(p-1)^2 r} \\
&\equiv (m_k^{-k(p-1)} m_{p-1}^{p-1})^r m_{p-1}^{(p-1)^2 r} \equiv m_{p-1}^{rp(p-1)} m_k^{-kr(p-1)} \\
&\equiv m_k^{-(p-1)^2} \pmod{p^2}.
\end{aligned}$$

Now $a^{(p-1)^2} \equiv a^{-(p-1)} \pmod{p^2}$. Hence, $m_k^{-(p-1)^2} \equiv m_k^{p-1} \pmod{p^2}$.

The basic tool which will be used in this paper is a result of Westlund [7] describing the integral basis for any pure field in question. It can be stated in the following form:

(1) If $Q(\sqrt[p]{m})$ is of class A, then $(1, a_1, a_2, \ldots, a_{p-1})$ is an integral basis, and if $Q(\sqrt[p]{m})$ is of class B, then $(\gamma, a_1, a_2, \ldots, a_{p-1})$ is an integral basis,

$$\gamma = \frac{1}{p}(a_1^{p-1} + ba_1^{p-2} + \ldots + b^{p-2}a_1 + 1),$$

and

$$a_i = (m_1^{i_1} m_2^{i_2} \ldots m_{p-1}^{i_{p-1}})^{1/p},$$

where $i_s \equiv si \pmod{p}$, $0 < i_s < p$, $1 \leqslant s \leqslant p-1$, $1 \leqslant i \leqslant p-1$, $b = m_1^1 m_2^2 \ldots m_{p-2}^{p-2}$, and $m = m_1^1 m_2^2 \ldots m_{p-1}^{p-1}$.

In this paper we prove the following general theorem:

THEOREM 2. *For any prime p, there exist only finitely many pure extensions of degree p which may contain F-sequences of length greater than 2.*

We also give the proof that $m(K) = 2$ if K is a pure cubic field different from $Q(\sqrt[3]{2})$, $Q(\sqrt[3]{5})$, $Q(\sqrt[3]{28})$, $Q(\sqrt[3]{62})$ and $Q(\sqrt[3]{109})$. The only exceptional case that will be treated is $Q(\sqrt[3]{2})$, where we give a proof of A. Schinzel that $Q(\sqrt[3]{2})$ contains exactly four basal F-sequences of length 4 and none of length greater than 4.

For pure fields of degree 5 and of class A, we have the following result:

THEOREM 3. *If K is any pure field of degree 5 and of class A different from $Q(\sqrt[5]{2^i 3^j})$, where $0 \leqslant i, j \leqslant 4$, and $i + j > 0$, then $m(K) = 2$.*

In the proof of Theorem 3 we use the following curious observation:

(2) If $K = Q(\sqrt[p]{m})$ is of class A with $m \equiv 0 \pmod{p}$, then $m(K) > 2$ implies $2^p \equiv 2 \pmod{p^2}$.

THEOREM 4. *If K is of class A, then the norm modulo p is a homomorphism from the ring of integers of K onto Z_p, the ring of residue classes modulo p.*

COROLLARY. *A pure field of degree $p > 3$ and of class A does not contain two units with the sum equal to another unit.*

As we easily see from Theorem 1, the Corollary implies that any field K of class A and of degree greater than 3 must contain a principal ideal of norm 2 if $m(K) > 2$. This is, of course, the case where $K = Q(\sqrt[p]{2})$. It could be interesting to decide when pure extension contains a principal ideal of norm 2. (**P 894**)

Lemmas 3-9 will help us to establish some useful features of the norm forms in pure extensions of prime degree.

LEMMA 3. *If* $n_1\zeta_p + n_2\zeta_p^2 + \ldots + n_{p-1}\zeta_p^{p-1} \in Z$ *with* $n_i \in Z$ *for all* i, $1 \leqslant i \leqslant p-1$, *then* $n_1 = n_2 = \ldots = n_{p-1}$.

Proof. The minimal polynomial $f(x) = 1 + x + x^2 + \ldots + x^{p-1}$ of ζ_p is of degree $p-1$. Since, clearly, any polynomial of degree $p-1$ vanishing for $x = \zeta_p$ is proportional to $f(x)$, the lemma follows.

LEMMA 4. *If* $\sum_{i=1}^{M} \zeta_p^{k_i} \in Z$ *with* $M \equiv 0 \pmod{p}$, *then*

$$\sum_{i=1}^{M} \zeta_p^{k_i} \equiv 0 \pmod{p}.$$

Proof. We have

$$\sum_{i=1}^{M} \zeta_p^{k_i} = n_0 + n_1\zeta_p + n_2\zeta_p^2 + \ldots + n_{p-1}\zeta_p^{p-1} = l,$$

$$\sum_{i=0}^{p-1} n_i = M, \quad n_i \in Z,\ 0 \leqslant i \leqslant p-1,\ l \in Z,$$

whence $n_1 = n_2 = \ldots = n_{p-1}$ by Lemma 2, and

$$\sum_{i=1}^{M} \zeta_p^{k_i} = n_0 + n_1(\zeta_p + \zeta_p^2 + \ldots + \zeta_p^{p-1}) = n_0 - n_1.$$

Now,

$$M = \sum_{i=0}^{p-1} n_i = n_0 + (p-1)n_1 \equiv 0 \pmod{p}$$

and

$$n_0 + (p-1)n_1 \equiv n_0 - n_1 \pmod{p}.$$

Hence

$$\sum_{i=1}^{M} \zeta^{k_i} = 0 \pmod{p}$$

and Lemma 4 follows.

LEMMA 5. *There is*

$$\prod_{i=0}^{p-1} (y_0 + y_1\zeta_p^i + y_2\zeta_p^{2i} + \ldots + y_{p-1}\zeta_p^{(p-1)i}) = y_0^p + y_1^p + \ldots + y_{p-1}^p + pF(y_0, y_1, \ldots, y_{p-1}),$$

where $F(y_0, y_1, \ldots, y_{p-1})$ *is a homogeneous polynomial of degree* p *in* $y_0, y_1, \ldots, y_{p-1}$ *with integer coefficients such that at least two* y_i*'s occur in each term.*

Proof. By taking the product, we get $y_0^p+y_1^p+\ldots+y_{p-1}^p+$ $+H(y_0, y_1, \ldots, y_{p-1})$ with every term of H of the form

$$\Big(\sum_{j=1}^{M}\zeta_p^{kj}\Big)(y_0^{i_0}y_1^{i_1}\ldots y_{p-1}^{i_{p-1}}), \qquad \sum_{j=1}^{M}\zeta_p^{kj}\in Z,\ 0\leqslant i_s\leqslant p-1,\ \sum_{s=0}^{p-1}i_s=p.$$

Clearly, at least two i_s's are different from 0, say $i_{s'}$ and $i_{s''}$. Since

$$M=\binom{p}{i_{s'}}\binom{p-i_{s'}}{i_{s''}}\ldots$$

and p is prime,

$$\binom{p}{i_{s'}}\equiv 0 \pmod{p}.$$

Consequently, $M\equiv 0 \pmod{p}$. Lemma 4 applies and the proof of Lemma 5 is complete.

Lemma 6. *If* $(\sqrt[p]{m^*\psi})\in Z$ *with* $m\in Z$ *and* ψ *an algebraic integer, then* $\sqrt[p]{m^*\psi})\equiv 0 \pmod{m^*}$.

Proof. $(\sqrt[p]{m^*\psi})\in Z$ implies that $(\sqrt[p]{m^*\psi})^p=m^*\psi^p\in Z$, and so $\psi^p\in Q$. Since ψ is an algebraic integer, it follows that $\psi^p\in Z$. Hence, every prime dividing m^* must divide $\sqrt[p]{m^*\psi}$ and the lemma follows.

We are now able to establish some properties of the norm form. Let a be an integer of K. If K is of class A, then, by (1), $a=x_0+x_1a_1+$ $+\ldots+x_{p-1}a_{p-1}$ with $x_i\in Z$. Thus

$$N(a)=\prod_{i=0}^{p-1}(x_0+\zeta_p^i x_1a_1+\zeta_p^{2i}x_2a_2+\ldots).$$

Substituting x_ia_i for y_i, $a_0=1$, Lemma 5 applies and we get

$$N(a)=x_0^p+(a_1x_1)^p+\ldots+(a_{p-1}x_{p-1})^p+pF(x_0a_0, x_1a_1, \ldots, x_{p-1}a_{p-1}),$$

where at least two x_ia_i occur in each term of F. Since $a_i/\sqrt[p]{m^*}$ is an algebraic integer for each i, $1\leqslant i\leqslant p-1$, we have, clearly,

$$pF(x_0a_0, x_1a_1, \ldots, x_{p-1}a_{p-1})=p\sqrt[p]{m^*\psi},$$

where $\psi(x_0, x_1, \ldots, x_{p-1})$ is an algebraic integer for all $(x_0, x_1, \ldots, x_{p-1})\in Z^p$. The expression

$$\frac{1}{p}\left(N(a)-\left(\sum_{i=1}^{p-1}(a_ix_i)^p\right)-x_0^p\right)=F(x_0a_0, x_1a_1, \ldots, x_{p-1}a_{p-1})=\sqrt[p]{m^*\psi}$$

is a rational number, and so a rational integer for all $(x_0, x_1, \ldots, x_{p-1}) \in Z^p$. Hence Lemma 6 applies and we get

If K is of class A, and $\alpha = x_0 + x_1\alpha_1 + \ldots + x_{p-1}\alpha_{p-1}$, then

$$N(\alpha) = x_0^p + x_1^p\alpha_1^p + \ldots + x_{p-1}^p\alpha_{p-1}^p + pm^*\psi'(x_0, x_1, \ldots, x_{p-1}) \tag{3}$$

with $\psi'(x_0, x_1, \ldots, x_{p-1})$ integer for all $(x_0, x_1, \ldots, x_{p-1}) \in Z^p$.

If K is of class B,

$$\alpha = \frac{x_0\left(1 + \sum_{i=1}^{p-1} a_1^i b^{p-i-1}\right)}{p} + x_1\alpha_1 + \ldots + x_{p-1}\alpha_{p-1} \quad \text{with } x_i \in Z.$$

We have

$$\alpha p = x_0\left(1 + \sum_{i=1}^{p-1} a_1^i b^{p-i-1}\right) + px_1\alpha_1 + \ldots + px_{p-1}\alpha_{p-1}.$$

Now

$$a_1^i = (m_1^i m_2^{2i} \ldots m_{p-1}^{(p-1)i})^{1/p} = \left(\prod_{s=1}^{p-1} m_s^{is}\right)^{1/p}.$$

Since, by (1), $i_s \equiv is \pmod p$, $i_s + \lambda_{is}p = is$ with $\lambda_{is} \in Z$. Hence

$$a_1^i = \left(\prod_{s=1}^{p-1} m_s^{i_s}\right)^{1/p}\left(\prod_{s=1}^{p-1} m_s^{\lambda_{is}}\right) = \alpha_i\left(\prod_{s=1}^{p-1} m_s^{\lambda_{is}}\right)$$

and

$$\sum_{i=1}^{p-1} a_1^i b^{p-1-i} = \sum_{i-1}^{p-1} \alpha_i\left(\prod_{s=1}^{p-1} m_s^{\lambda_{is}}\right) b^{p-1-i}.$$

Put, for abbreviation,

$$\left(\prod_{s=1}^{p-1} m_s^{\lambda_{is}}\right) b^{p-1-i} = b_i.$$

We get

$$\alpha p = x_0 + (px_1 + x_0 b_1)\alpha_1 + \ldots + (px_{p-1} + x_0 b_{p-1})\alpha_{p-1}.$$

With $y_i = px_i + x_0 b_i$ and $y_0 = x_0$, the same argument as in (3) applies and we get

$$\begin{aligned} N(\alpha p) &= p^p N(\alpha) \\ &= y_0^p + y_1^p\alpha_1^p + \ldots + y_{p-1}^p\alpha_{p-1}^p + pm^*\psi'(y_0, y_1, \ldots, y_{p-1}) \end{aligned} \tag{4}$$

with $\psi'(y_0, y_1, \ldots, y_{p-1})$ integer for all $(y_0, y_1, \ldots, y_{p-1}) \in Z^p$.

Suppose that a pure field K of prime degree contains an F-sequence of length greater than 2. Since every initial segment of an F-sequence is also an F-sequence, K contains an F-sequence of length 3. By Lemma 1,

it also contains a basal F-sequence of length 3, say $\langle 0, 1, a_3\rangle$. Theorem 1 immediately implies

$$|N(a_3)| \leqslant 2 \quad \text{and} \quad |N(a_3-1)| \leqslant 2. \tag{5}$$

Our method will now consist in assigning a congruence system dependent on the class of K to every pair of values $\langle N(a_3), N(a_3-1)\rangle$. The following lemmas will considerably diminish the number of classes to be investigated.

LEMMA 7. *For all a in real pure extensions of odd degree, we have* $\operatorname{sgn} N(a) = \operatorname{sgn} a$.

Proof. We have $N(a) = aa^{(1)}a^{(2)} \dots a^{(n)}$, where $a^{(i)}$, $1 \leqslant i \leqslant n$, denote the conjugates of K. Since every complex number appears in the product together with its complex conjugate, the lemma follows.

LEMMA 8. *For all algebraic number fields K of odd degree, the following statements are equivalent*:

(i) *There exists an $a \in K$ such that $\langle N(a), N(a-1)\rangle = \langle a, b\rangle$.*

(ii) *There exists a $\beta \in K$ such that $\langle N(\beta), N(\beta-1)\rangle = \langle -b, -a\rangle$.*

Proof. Suppose that $\langle N(a), N(a-1)\rangle = \langle a, b\rangle$ and put $\beta = 1-a$. Then $N(1-a) = -N\big(-(1-a)\big) = -N(a-1) = -b$, and $N(1-a-1) = N(-a) = -a$, since K is of odd degree. Thus (i) implies (ii). Conversely, suppose that $\langle N(\beta), N(\beta-1)\rangle = \langle -b, -a\rangle$ and put $a = 1-\beta$. Clearly, $N(a) = a$ and $N(a-1) = b$. Thus (ii) implies (i).

LEMMA 9. *For all odd primes p,*

$$\begin{aligned} &\big(x^p-2, (x-1)^p-2\big) = 1, \quad \big(x^p-2, (x-1)^p-1\big) = 1,\\ &\big(x^p-2, (x-1)^p+1\big) = 1, \quad \big(x^p-2, (x-1)^p+2\big) = 1,\\ &\big(x^p-1, (x-1)^p-2\big) = 1, \quad \big(x^p-1, (x-1)^p-1\big) = 1,\\ &\big(x^p-1, (x-1)^p+1\big) = 1. \end{aligned}$$

Proof. If one of the numbers a and b is equal to ± 2 and the other is equal to ± 1, the polynomials x^p-a and $(x-1)^p-b$ are coprime, since exactly one of them is irreducible.

a. $\big(x^p-2, (x-1)^p-2\big) = 1$.

For if $x^p-2 = 0$, then $x = \sqrt[p]{2}\,\zeta_p^i$, and so $\big(\sqrt[p]{2}\,\zeta_p^i-1\big)^p = 2$ would imply that $\sqrt[p]{2}\,\zeta_p^i - 1 = \sqrt[p]{2}\,\zeta_p^j$. Hence $\sqrt[p]{2}\,(\zeta_p^i-\zeta_p^j) = 1$, a contradiction.

b. $\big(x^p-2, (x-1)^p+2\big) = 1$.

Assuming the contrary we get, by the same argument, $\sqrt[p]{2}\,\zeta_p^i + \sqrt[p]{2}\,\zeta_p^j = 1$, a contradiction.

c. $\big(x^p-1, (x-1)^p-1\big) = 1$.

For $x^p = 1$ implies $x = \zeta_p^i$ and $(x-1)^p = 1$ implies $x-1 = \zeta_p^j$. Hence $\zeta_p^i - \zeta_p^j = 1$, a contradiction.

d. $(x^p-1, (x-1)^p+1) = 1$.

Assuming the contrary we get, by a similar argument, $\zeta_p^i + \zeta_p^j = 1$, a contradiction.

Clearly, we have

$$(6)\quad (x^p-a, (x-1)^p-b) = 1 \quad \text{iff} \quad (x^p-p^pa, (x-p)^p-p^pb) = 1.$$

Since, clearly, $a_i^p \equiv 0 \pmod{m^*}$ for all i, $1 \leqslant i \leqslant p-1$, (3) and (4) give

$$(7)\quad N(a) \equiv x_0^p \pmod{m^*} \quad \text{if } K \text{ is of class } A,$$

$$(8)\quad p^pN(a) \equiv x_0^p \pmod{m^*} \quad \text{if } K \text{ is of class } B.$$

Suppose that K contains an F-sequence of length greater than 2. Then, as we have already shown in (5), we may suppose that K contains an F-sequence $\{a_i\}$ subject to $|N(a_3)| \leqslant 2$ and $|N(a_3-1)| \leqslant 2$. Moreover, since all terms in an F-sequence are distinct and the norm of an algebraic integer is 0 if and only if the integer is 0, we are left with the possibilities

$$-2 \leqslant N(a_3) < 0, \quad 0 < N(a_3) \leqslant 2, \quad -2 \leqslant N(a_3-1) < 0,$$
$$0 < N(a_3-1) \leqslant 2.$$

By Lemma 7, we may exclude all pairs of values $\langle N(a_3), N(a_3-1)\rangle$ such that $N(a_3-1) > 0$ and $N(a_3) < 0$, since, otherwise, $\operatorname{sgn} N(a_3-1) = 1 = \operatorname{sgn}(a_3-1)$ and $\operatorname{sgn} N(a_3) = -1$ implies $\operatorname{sgn} a_3 = -1 = \operatorname{sgn}(a_3-1)$.

By Lemma 8, $\langle N(a), N(a-1)\rangle = \langle a, b\rangle$ yields the same conclusions about K as $\langle N(\beta), N(\beta-1)\rangle = \langle -b, -a\rangle$. Hence it is sufficient to consider $\langle N(a_3), N(a_3-1)\rangle$ such that $N(a_3)+N(a_3-1) \geqslant 0$.

All these considerations leave us with the following cases:

$$(9)\quad \langle N(a_3), N(a_3-1)\rangle$$
$$= \langle 2,2\rangle, \langle 2,1\rangle, \langle 1,2\rangle, \langle 1,1\rangle, \langle 2,-1\rangle, \langle 2,-2\rangle, \langle 1,-1\rangle.$$

For every pair of values, we have the congruence systems. Namely, if $a_3 = x_0 + \ldots + x_{p-1}a_{p-1}$, we have the system

$$(10)\quad x_0^p \equiv N(a_3) \pmod{m^*}, \quad (x_0-1)^p \equiv N(a_3-1) \pmod{m^*}$$

derived from (7) and (1); and, if

$$a_3 = \frac{x_0}{p} + \ldots + \frac{(px_{p-1} + x_0b_{p-1})a_{p-1}}{p},$$

we have the system

$$(11)\quad x_0^p \equiv N(a_3)p^p \pmod{m^*}, \quad (x_0-p)^p \equiv N(a_3-1)p^p \pmod{m^*}$$

derived from (8) and (1).

Proof of Theorem 2. The theorem is true when $p = 2$ (it follows from the unpublished work of Wańtuła). If p is an odd prime, then (10), (11) and a well-known identity (see [6], p. 106) imply that m^* must divide the resultant of the corresponding pair of polynomials

$$\langle x_0^p - N(a_3), (x_0-1)^p - N(a_3-1)\rangle$$

or

$$\langle x_0^p - p^p N(a_3), (x_0-p)^p - p^p N(a_3-1)\rangle.$$

From Lemma 9 and formula (6) it follows that the resultant is different from 0. Therefore, the divisibility can hold only for finitely many values of m^*. To every m^* there correspond finitely many fields and Theorem 2 follows.

Proof of Theorem 4. We develop $N(\alpha+\beta)$ using (3) and, for

$$\alpha = x_0 + x_1 a_1 + \ldots + x_{p-1} a_{p-1},$$

$$\beta = y_0 + y_1 a_1 + \ldots + y_{p-1} a_{p-1},$$

we get

$$N(\alpha+\beta) \equiv (x_0+y_0)^p + (x_1+y_1)^p a_1^p + \ldots + (x_{p-1}+y_{p-1})^p a_{p-1}^p \pmod p.$$

Hence

$$\begin{aligned} N(\alpha+\beta) &\equiv x_0^p + y_0^p + x_1^p a_1^p + y_1^p a_1^p + \ldots + x_{p-1}^p a_{p-1}^p + y_{p-1}^p a_1^p \\ &\equiv N(\alpha) + N(\beta) \pmod p. \end{aligned}$$

The norm is onto modulo p since if $a \in Z$, then $N(a) = a^p \equiv a \pmod p$. The homomorphism property under multiplication follows directly from $N(\alpha\beta) = N(\alpha)N(\beta) \equiv N(\alpha)N(\beta) \pmod p$, and the proof of the theorem is complete.

Proof of the Corollary. If α and β are units, then

$$N(\alpha+\beta) \equiv N(\alpha) + N(\beta) \equiv 0, 2-2 \pmod p$$

and the Corollary follows.

Theorem 4 implies that if $a_3 \in K$ and K is of class A, then

$$N(a_3-1) \equiv N(a_3) - 1 \pmod p. \tag{12}$$

The only pairs listed in (9) satisfying (12) are $\langle 2, 1\rangle$ if $p > 3$ and $\langle 2, 1\rangle$ and $\langle 2, -2\rangle$ if $p = 3$. We have

(13) If K is a pure field of class A that contains an F-sequence of length greater than 2, say $\langle 0, 1, a_3\rangle$, then

$$a_3 = \sum_{i=0}^{i=p-1} x_i a_i \qquad (a_0 = 1)$$

must satisfy the following conditions:

$$(14)\qquad x_0^p \equiv 2 \pmod{m^*}, \quad (x_0-1)^p \equiv 1 \pmod{m^*} \quad \text{if } p > 3$$

or

$$(15)\qquad x_0^p \equiv 2 \pmod{m^*}, \quad (x_0-1)^p \equiv -2 \pmod{m^*} \quad \text{if } p = 3.$$

Suppose that $K = Q(\sqrt[p]{m})$ is of class A and contains an F-sequence of length greater than 2 with $m \equiv 0 \pmod{p}$. First of all, (13) applies and we have $\langle 0, 1, a_3\rangle$ as a basal F-sequence in K, $a_3 = x_0 + x_1 a_1 + \ldots + x_{p-1} a_{p-1}$, and a_3 satisfies the following conditions:

$N(a_3) = 2$ and $N(a_3-1) = 1$ if $p > 3$, or

$N(a_3) = 2$ and $N(a_3-1) = -2$ if $p = 3$.

We have, by (3),

$$N(a_3) = 2 = x_0^p + x_1^p a_1^p + \ldots + x_{p-1}^p a_{p-1}^p + pm^* \psi'(x_0, x_1, \ldots, x_{p-1})$$

where $\psi'(x_0, x_1, \ldots, x_{p-1})$ is integer for all $(x_0, x_1, \ldots, x_{p-1}) \in Z^p$. Since $m \equiv 0 \pmod{p}$, $m^* \equiv 0 \pmod{p}$. Hence we have the congruences

$$(16)\qquad \begin{aligned} x_0^p + pF(x_1, x_2, \ldots, x_{p-1}) &\equiv 2 \pmod{p^2}, \\ (x_0-1)^p + pF(x_1, x_2, \ldots, x_{p-1}) &\equiv 1 \pmod{p^2}, \end{aligned}$$

where $F(x_1, x_2, \ldots, x_{p-1}) \in Z$, or

$$(17)\qquad \begin{aligned} x_0^3 + 3G(x_1, x_2) &\equiv 2 \pmod{9}, \\ (x_0-1)^3 + 3G(x_1, x_2) &\equiv -2 \pmod{9}, \end{aligned}$$

where $G(x_1, x_2) \in Z$. However, (17) is inconsistent, since $x_0^3 + 3G(x_1, x_2) \equiv 2 \pmod{9}$ implies $x_0 \equiv 2 \pmod{3}$, and so $3G(x_1, x_2) \equiv 3 \pmod{9}$. However, the congruence $(x_0-1)^3 + 3G(x_1, x_2) \equiv -2 \pmod{9}$ implies $3G(x_1, x_2) \equiv 6 \pmod{9}$. Congruences (16) imply $x_0 \equiv 2 \pmod{p}$, and so

$$(x_0-1)^p + pF(x_1, x_2, \ldots, x_{p-1}) \equiv 1 \pmod{p^2}$$

yields

$$pF(x_1, x_2, \ldots, x_{p-1}) \equiv 0 \pmod{p^2}.$$

Hence $x_0^p \equiv 2^p \equiv 2 \pmod{p^2}$, which proves the assertion in (2).

$p = 3$.

A. Suppose that K is a pure cubic field of class A. Then (13) applies and we get

$$(18)\qquad \begin{aligned} x_0^3 &\equiv 2 \pmod{m^*}, \\ (x_0-1)^3 &\equiv 1 \pmod{m^*}, \end{aligned} \quad \text{or} \quad \begin{aligned} x_0^3 &\equiv 2 \pmod{m^*}, \\ (x_0-1)^3 &\equiv -2 \pmod{m^*}. \end{aligned}$$

These two systems imply $m^* = 2$ or $m^* = 5$ with the corresponding fields $Q(\sqrt[3]{2})$ and $Q(\sqrt[3]{5})$.

B. Suppose that K is a pure cubic field of class B. By (11), we have the following congruence system:

$$(19)\quad x_0^3 \equiv 27N(a_3) \pmod{m^*}, \qquad (x_0-3)^3 \equiv 27N(a_3-1) \pmod{m^*}.$$

We have $m^* = m_1 m_2$ and, since K is of class B, $m_1^2 \equiv m_2^2 \pmod 9$. Hence $m^* \not\equiv 0 \pmod 3$, and (19) reduces to

$$(20)\qquad x_0^3 \equiv 27\alpha \pmod{m^*}, \qquad x_0^2 - 3x_0 \equiv 3\beta \pmod{m^*},$$

where $\alpha = N(a_3)$ and $\beta = N(a_3) - N(a_3-1) - 1$. It follows that $x_0^3 \equiv 3x_0^2 + 3\beta x_0 \equiv 27\alpha \pmod{m^*}$, whence $x_0^2 + \beta x_0 \equiv 9\alpha \pmod{m^*}$. Since $x_0^2 - 3x_0 \equiv 3\beta \pmod{m^*}$, we get

$$(\beta+3)x_0 \equiv 9\alpha - 3\beta \pmod{m^*}.$$

Thus $(\beta+3)^2 x_0^2 \equiv 9(3\alpha-\beta)^2 \pmod{m^*}$ and, since

$$(\beta+3)^2 x_0^2 \equiv 3(\beta+3)^2 x_0 + 3\beta(\beta+3)^2 \pmod{m^*},$$

it follows that

$$9(3\alpha-\beta)^2 - 3(\beta+3)\cdot 3(3\alpha-\beta) - 3\beta(\beta+3)^2 = \psi'(\alpha,\beta) \equiv 0 \pmod{m^*}.$$

Since $m \not\equiv 0 \pmod 3$, we have

$$\psi'(\alpha,\beta) = 3(3\alpha-\beta)^2 - (\beta+3)\cdot 3(3\alpha-\beta) - \beta(\beta+3)^2 \equiv 0 \pmod{m^*}.$$

The following table gives the values of $\psi'(\alpha,\beta)$, when $\langle N(a_3), N(a_3-1)\rangle$ takes the values given in (9):

$N(a_3-1)$	α	β	$\psi'(\alpha,\beta)$	$N(a_3-1)$	α	β	$\psi'(\alpha,\beta)$
2	2	−1	109	−1	2	2	−62
2	1	−2	62	−1	1	1	−28
1	2	0	54	−2	2	3	−135
1	1	−1	28				

Of these values only m^* equal to 109, 62 and 28 correspond to fields of class B. The corresponding fields are $Q(\sqrt[3]{109})$, $Q(\sqrt[3]{62})$ and $Q(\sqrt[3]{28})$.

Now we consider in detail the case of $K = Q(\sqrt[3]{2})$.

LEMMA 10. *Let* $\eta = \sqrt[3]{2}$. *All integral solutions of the equations*

(a) $\eta(1+\eta+\eta^2)^n - (1+\eta+\eta^2)^m = 1$,

(b) $(\eta+1)(1+\eta+\eta^2)^n - \eta(1+\eta+\eta^2)^m = 1$,

(c) $\eta^2(1+\eta+\eta^2)^n - (\eta+1)(1+\eta+\eta^2)^m = 1$,

(d) $\eta^2(1+\eta+\eta^2)^n + (\eta+1)(1+\eta+\eta^2)^m = 1$

are $n = m = 1$ *or* $n = 0$, $m = -1$ *for* (a); $n = m = 0$ *for* (b); $n = 0$, $m = -1$ *for* (c); *and* $n = m = -1$ *for* (d).

Proof. If $m \geqslant 0$, then

$$\eta(1+\eta+\eta^2)^n-(1+\eta+\eta^2)^m$$
$$=(1+\eta+\eta^2)^m[\eta(1+\eta+\eta^2)^{n-m}-1]\begin{cases}>1 & \text{if } n>m,\\ =(1+\eta+\eta^2)^{m-1} & \text{if } n=m,\\ <0 & \text{if } n<m;\end{cases}$$

$$(\eta+1)(1+\eta+\eta^2)^n-\eta(1+\eta+\eta^2)^m$$
$$=(1+\eta+\eta^2)^m[(\eta+1)(1+\eta+\eta^2)^{n-m}-\eta]\begin{cases}>1 & \text{if } n>m,\\ =(1+\eta+\eta^2)^m & \text{if } n=m,\\ <0 & \text{if } n<m;\end{cases}$$

$$\eta^2(1+\eta+\eta^2)^n-(\eta+1)(1+\eta+\eta^2)^m$$
$$=(1+\eta+\eta^2)^m[\eta^2(1+\eta+\eta^2)^{n-m}-\eta-1]\begin{cases}>1 & \text{if } n>m,\\ <0 & \text{if } n\leqslant m;\end{cases}$$

$$\eta^2(1+\eta+\eta^2)^n+(\eta+1)(1+\eta+\eta^2)^m>1.$$

Thus (a) implies $m=n=1$, (b) implies $m=n=0$, and (c) and (d) are impossible.

If $m<0$, then

$$\eta(1+\eta+\eta^2)^n-1\begin{cases}>(1+\eta+\eta^2)^m & \text{if } n>0,\\ =(1+\eta+\eta^2)^{-1} & \text{if } n=0,\\ <0 & \text{if } n<0;\end{cases}$$

$$(\eta+1)(1+\eta+\eta^2)^n-1\begin{cases}>\eta(1+\eta+\eta^2)^m & \text{if } n\geqslant 0,\\ <0 & \text{if } n<0;\end{cases}$$

$$\eta^2(1+\eta+\eta^2)^n-1\begin{cases}>(\eta+1)(1+\eta+\eta^2)^m & \text{if } n>0,\\ =(\eta+1)(1+\eta+\eta^2)^{-1} & \text{if } n=0,\\ <0 & \text{if } n<0;\end{cases}$$

$$\eta^2(1+\eta+\eta^2)^n+(\eta+1)(1+\eta+\eta^2)^m\begin{cases}>1 & \text{if } n\geqslant 0,\\ =1+(\eta+1)[(1+\eta+\eta^2)^m- & \\ \quad -(1+\eta+\eta^2)^{-1}] & \text{if } n=-1,\\ <1 & \text{if } n<-1.\end{cases}$$

Thus (a) implies $n=0$, $m=-1$, (b) is impossible, (c) implies $n=0$, $m=-1$, and (d) implies $n=m=-1$.

Let $Q(\sqrt[3]{2})$ contain an F-sequence of length 5, say $\langle 0, 1, a_3, a_4, a_5\rangle$, with $a_j=x_j+y_j\eta+z_j\eta^2$; $x_j, y_j, z_j \in Z$. Since $x_j^2-x_j \equiv 0 \pmod 2$, we get,

by (12), $N(a_j-1) \equiv N(a_j)-1 \pmod 6$. Therefore,

(e) $N(a_j-1) = N(a_j)-1$, or

(f) $N(a_j-1) = N(a_j)-7$, or

(g) $N(a_j-1) = N(a_j)+5$, or

(h) $|N(a_j-1)-N(a_j)|+1 \geqslant 12$.

In view of $|N(a_j)| \leqslant j-1$ and $|N(a_j-1)| \leqslant j-1$, (e) gives

(i) $N(a_j) = 2$, $N(a_j-1) = 1$ or $N(a_j) = -1$, $N(a_j-1) = -2$ for $3 \leqslant j \leqslant 5$, or

(j) $N(a_j) = 3$, $N(a_j-1) = 2$ or $N(a_j) = -2$, $N(a_j-1) = -3$ for $4 \leqslant j \leqslant 5$, or

(k) $N(a_j) = 4$, $N(a_j-1) = 3$ or $N(a_j) = -3$, $N(a_j-1) = -4$ for $j = 5$.

Relation (f) gives $7 \leqslant 2(j-1)$, and

(l) $N(a_j) = 4$, $N(a_j-1) = -3$ or $N(a_j) = 3$, $N(a_j-1) = -4$ $(j = 5)$.

Equality (g) implies $N(a_j) < 0 < N(a_j-1)$ and, by Lemma 7, $a_j < 0 < a_j-1$ which is impossible.

Inequality (h) implies $11 \leqslant 2(j-1)$, $j \geqslant 7$, which is also impossible.

Thus we are left with (i), (j), (k) or (l).

It follows from the table of Delone and Faddeev [2] that $1+\eta+\eta^2$ is the fundamental unit of $Q(\sqrt[3]{2})$; moreover, the equalities $(2) = (\eta)^3$ and $(3) = (\eta+1)^3$ show that (η) and $(\eta+1)$ are the only ideals of $Q(\sqrt[3]{2})$ with norms 2 and 3, respectively. Therefore,

(i) gives $a_j = \eta(1+\eta+\eta^2)^n$ or $-(1+\eta+\eta^2)^m$ $(3 \leqslant j \leqslant 5)$, where m and n satisfy (a);

(j) gives $a_j = (1+\eta)(1+\eta+\eta^2)^n$ or $-\eta(1+\eta+\eta^2)^m$ $(4 \leqslant j \leqslant 5)$, where m and n satisfy (b);

(k) gives $a_j = \eta^2(1+\eta+\eta^2)^n$ or $(1+\eta)(1+\eta+\eta^2)^m$ $(j = 5)$, where m and n satisfy (c).

(l) gives $a_j = \eta^2(1+\eta+\eta^2)^n$ or $(1+\eta)(1+\eta+\eta^2)^m$ $(j = 5)$, where m and n satisfy (d).

In virtue of Lemma 10, this implies

$a_j = \eta,\ 2+\eta+\eta^2,\ 1-\eta,\ -1-\eta-\eta^2$ $(3 \leqslant j \leqslant 5)$, or

$a_j = 1+\eta,\ -\eta$ $(4 \leqslant j \leqslant 5)$, or

$a_j = \eta^2,\ 1-\eta^2,\ 2-\eta^2,\ \eta^2-1$ $(j = 5)$.

The conditions $0 < |N(a_3)|$, $|N(a_3-1)| \leqslant 2$, $0 < |N(a_4-a_3)| \leqslant 3$ and $0 < |N(a_5-a_3)| \leqslant 4$, $a_5 \neq a_4$, imply that there are only four possibilities for $\langle a_3, a_4, a_5\rangle$, namely

$$\langle \eta, 1+\eta, \eta^2 \rangle, \quad \langle 2+\eta+\eta^2, -1-\eta-\eta^2, -\eta \rangle,$$

$$\langle 1-\eta, -\eta, 1-\eta^2 \rangle, \quad \langle -1-\eta-\eta^2, 2+\eta+\eta^2, 1+\eta \rangle.$$

However, in each of these cases $|N(a_5-a_4)| = 5$, which proves that there is no F-sequence of length 5 in $Q(\sqrt[3]{2})$.

Proof of Theorem 3. Suppose that $p = 5$ and K is of class A. If K contains an F-sequence of length greater than 2, then (13) holds and we have

$$x_0^5 \equiv 2 \pmod{m^*}, \quad (x_0-1)^5 \equiv 1 \pmod{m^*}. \tag{21}$$

Since the resultant of x_0^5-2 and $(x_0-1)^5-1$ is $\pm 2\cdot 3\cdot 5^5$, it follows that m^* equal to 2, 3, 5, $2\cdot 3$, $2\cdot 5$, $3\cdot 5$ or $2\cdot 3\cdot 5$. Now, since $2^5 \not\equiv 2 \pmod{5^2}$, we have, by (2), $m \not\equiv 0 \pmod 5$, and whence $m^* \not\equiv 0 \pmod 5$. Hence $m^* = 2$, 3 or $2\cdot 3$. If m^* equal to 2, 3 and 6, then (21) is solvable. To these values of m^* there correspond the following fields:

$$Q(\sqrt[5]{2}), \; Q(\sqrt[5]{3}), \; Q(\sqrt[5]{2^i\cdot 3}), \quad 0 < i < 5.$$

This completes the proof of the theorem.

REFERENCES

[1] D. Barsky, *Sur les systèmes complets des restes modulo les idéaux d'un corps de nombres*, Acta Arithmetica 22 (1972), p. 49-56.

[2] B. N. Delone and D. K. Faddeev, *Theory of irrationalities of the third degree*, Providence 1964.

[3] E. Hecke, *Vorlesungen über die Theorie der algebraischen Zahlen*, New York 1948.

[4] J. Latham, *On sequences of algebraic integers*, Journal of the London Mathematical Society 6 (1973), p. 555-560.

[5] L. Siegel, *Algebraisch Abhängigkeit von Wurzeln*, Acta Arithmetica 21 (1972), p. 59-64.

[6] B. L. van der Waerden, *Algebra I*, Berlin - Heidelberg - New York 1966.

[7] J. Westlund, *On the fundamental number of the algebraic number field* $k(\sqrt[p]{m})$, Transactions of the American Mathematical Society 11 (1910), p. 388-392.

Reçu par la Rédaction le 6. 9. 1972