Journal of Mathematical Sciences, Vol. 98, No. 4, 2000

DIOPHANTINE REPRESENTATIONS OF LINEAR RECURRENT SEQUENCES. II

M. A. Vsemirnov UDC 511.5

Direct constructions of Diophantine representations for linear recurrent sequences are considered. Diophantine representations of the sets of values for third-order sequences with negative discriminants are found. As an auxiliary problem, we study the structure of the multiplicative group of the ring $\mathbf{Z}[\lambda]$, *where* λ *is an invertible algebraic integer (unit) in a real quadratic field or in a cubic field of negative discriminant. The index of the subgroup* $\{\pm\lambda^n \mid n \in \mathbf{Z}\}$ *in the group* $(\mathbf{Z}[\lambda])^*$ *and the generator of* $(\mathbf{Z}[\lambda])^*$ *are evaluated explicitly. Bibliography: 14 titles.*

1. Introduction

In the present paper, we continue to investigate the problem of constructing direct Diophantine representations of linear recurrent sequences set up in [12, Open question 2.3]. One can find the motivation of the problem and its detailed setting in the author's paper [3]. For the history of this problem, see [12, Chapter 2]. Most of the results of this series of papers were announced by the author in [2, 4, 5].

Let us recall the main definitions, constructions, and results of [3] that we need below.

Definition. *A set* $\mathcal{M}$ *of* n*-tuples of integers is called Diophantine if there exists a polynomial* $P(a_1, \dots, a_n, x_1, \dots, x_m)$ *with integer coefficients such that*

$$\langle a_1, \dots, a_n \rangle \in \mathcal{M} \Longleftrightarrow \exists x_1 \in \mathbf{N}, \dots, \exists x_m \in \mathbf{N}\ [P(a_1, \dots, a_n, x_1, \dots, x_m) = 0]. \tag{1}$$

We call equivalence (1) *a Diophantine representation of the set* $\mathcal{M}$.

Remark. As was proved by Matiyasevich in his fundamental work [11], the number-theoretic notion of a Diophantine set coincides with the notion of a recursively enumerable set. See also [12].

Traditionally, in the problems of constructing Diophantine representations one speaks about sets of n-tuples of *positive integers*. In our case, it is more natural to consider sets of n-tuples of integers, since the values of an arbitrary linear recurrent sequence can be both positive and negative. For the same reason, it will be convenient to consider $\mathbf{Z}$-Diophantine representations, i.e., representations analogous to (1), but with variables $x_1, x_2, \dots, x_m$ ranging over integers.

It is well known that the notions of Diophantine and $\mathbf{Z}$-Diophantine sets coincide (for example, see [12, §1.3]). More precisely, for a given Diophantine representation of a set one can find its $\mathbf{Z}$-Diophantine representation and vice versa. The same technique allows us to show that for a Diophantine set $\mathcal{M} \subset \mathbf{Z}^n$, the sets $\mathcal{M}' = \{\langle a_1, \dots, a_n \rangle \in \mathbf{N}^n : \exists \langle b_1, \dots, b_n \rangle \in \mathcal{M}\ [a_1 = |b_1|, \dots, a_n = |b_n|]\}$ and $\mathcal{M}'' = \mathcal{M} \cap \mathbf{N}^n$ are also Diophantine.

To avoid awkward formulas, we shall not transform $\mathbf{Z}$-Diophantine representations into the corresponding Diophantine representations. For the same reason, we consider systems of Diophantine equations. If necessary, one can transform any such system into a single Diophantine equation. In addition, we use simple relations such as divisibility and inequalities which are obviously Diophantine.

2. Recurrent sequences and their properties

Let a sequence a_n be defined by the following recurrent relation of order k (i.e., each member of the sequence is expressed as a linear combination of the k members directly preceding it):

$$a_{n+k} = b_{k-1}a_{n+k-1} + \dots + b_0 a_n, \tag{2}$$

Translated from *Zapiski Nauchnykh Seminarov POMI*, Vol. 241, 1997, pp. 5–29. Original article submitted October 10, 1997.

with the initial conditions

$$a_0 = 1, \quad a_{-1} = a_{-2} = \ldots = a_{-k+1} = 0. \tag{3}$$

We assume the coefficients b_i to be integer. Furthermore, we impose the additional restriction

$$b_0 = \pm 1. \tag{4}$$

This restriction allows us to define the given sequence for all negative values of n by the relation

$$a_n = (a_{n+k} - b_{k-1}a_{n+k-1} - \ldots - b_1 a_{n+1})/b_0 \tag{5}$$

and obtain an infinite (in both directions) *integer-valued* sequence. We restrict ourselves to such sequences.

Below we consider the case that is most interesting for applications, namely, the case where the polynomial

$$f(\lambda) = t^k - b_{k-1}t^{k-1} - \ldots - b_1 t - b_0 \tag{6}$$

is irreducible over $\mathbf{Q}$. As we see later, in the cases under consideration, we can express the irreducibility condition for f by a system of Diophantine equations in the variables $b_0, b_1, \ldots, b_{k-1}$.

A Diophantine representation of the linear recurrent sequence (2)–(3) means for us a Diophantine representation of the set

$$\mathcal{M} = \{\langle u, n\rangle \mid u = a_n\}. \tag{7}$$

Consider one simple case. Let the polynomial f defined by (6) be the lth cyclotomic polynomial; then the sequence under consideration is a periodic sequence with period not exceeding l. It is well known that for a polynomial f with k distinct roots $\lambda_{(1)} = \lambda$, $\lambda_{(2)}, \ldots, \lambda_{(k)}$, there exist coefficients c_j, $j = 1, \ldots k$, such that

$$a_n = \sum_{j=1}^{k} c_j \lambda_{(j)}^n.$$

For a cyclotomic polynomial, all the $\lambda_{(j)}$ are roots of unity. Hence, the sequence a_n is periodic. But for a periodic sequence (with fixed b_0, b_1, $\ldots$, b_{k-1}), the problem of constructing its Diophantine representation is trivial. Therefore, below we may exclude this case and assume that f is not a cyclotomic polynomial.

Let us recall the main construction introduced in [3]. Consider the following square matrices of size k (E denotes the identity matrix):

$$B = \begin{pmatrix} 0 & 0 & \ldots & 0 & b_0 \\ 1 & 0 & \ldots & 0 & b_1 \\ 0 & 1 & \ldots & 0 & b_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & b_{k-1} \end{pmatrix}, \tag{8}$$

$$\begin{aligned} A(x_0, x_1, \ldots, x_{k-1}) &= \sum_{l=0}^{k-1} x_l \left(B^l - \sum_{j=1}^{l} b_{k-j} B^{l-j} \right) \\ &= x_0 E + x_1(B - b_{k-1}E) + \ldots + x_{k-1}(B^{k-1} - b_{k-1}B^{k-2} - \ldots - b_1 E), \end{aligned} \tag{9}$$

$$A^*(n) = A(a_n, a_{n-1}, \ldots, a_{n-k+1}). \tag{10}$$

Define the following homogeneous polynomial of degree k in k variables:

$$F_B(x_0, x_1, \ldots, x_{k-1}) = \det A(x_0, x_1, \ldots, x_{k-1}). \tag{11}$$

As was proved in [3],

$$\begin{aligned} F_B(a_n, a_{n-1}, \ldots, a_{n-k+1}) &= \det B^n = (\pm b_0)^n = \pm 1, \\ F_B(-a_n, -a_{n-1}, \ldots, -a_{n-k+1}) &= \det(-B)^n = (\pm b_0)^n = \pm 1. \end{aligned} \tag{12}$$

The following problem naturally arises: when do these relations characterize the sequence under consideration completely?

Definition (see [3]). *We say that the relation*

$$F_B(x_0, x_1, \dots, x_{k-1}) = \pm 1 \tag{13}$$

is characteristic for sequence (2)–(3) *if Eq.* (13) *has no other integer solutions* $\langle x_0, x_1, \dots, x_{k-1}\rangle$ *than those listed in the following two series:*

$$\langle x_0, x_1, \dots, x_{k-1}\rangle = \langle a_n, a_{n-1}, \dots, a_{n-k+1}\rangle,$$

$$\langle x_0, x_1, \dots, x_{k-1}\rangle = \langle -a_n, -a_{n-1}, \dots, -a_{n-k+1}\rangle.$$

Classification of all sequences of the form (2)–(3) (in other words, of all sets of coefficients $b_0, b_1, \dots b_{k-1}$) for which relation (13) is characteristic is the first step towards the direct construction of a Diophantine representation of the set (7). In fact, if for a given set $b_0, b_1, \dots b_{k-1}$, relation (13) is characteristic for sequence (2)–(3), then one can easily find a **Z**-Diophantine representation of the set

$$\mathcal{M}_1 = \{u \in \mathbf{Z} \mid \exists n \in \mathbf{Z}\ [u = a_n \vee u = -a_n]\}.$$

Namely,

$$x \in \mathcal{M}_1 \iff \exists x_1 \in \mathbf{Z}, \dots, \exists x_{k-1} \in \mathbf{Z}\ [(F_B(x, x_1, \dots, x_{k-1}))^2 - 1 = 0].$$

3. General scheme

As is shown in [3, 4], the problem of description of all sequences for which relation (13) is characteristic is closely related to properties of units (invertible elements) in orders of algebraic numbers.

Let λ be a root of the polynomial f defined by (6). Since we assume f to be irreducible over $\mathbf{Q}$, the field $\mathbf{Q}(\lambda)$ is an extension of $\mathbf{Q}$ of degree k, $[\mathbf{Q}(\lambda) : \mathbf{Q}] = k$. Let $(\mathbf{Z}[\lambda])^*$ denote, as usual, the multiplicative group of order $(\mathbf{Z}[\lambda])$. Since $b_0 = \pm 1$, we have

$$\{\pm\lambda^n : n \in \mathbf{Z}\} \subseteq (\mathbf{Z}[\lambda])^*.$$

The following representation of powers of λ will be useful (see [3, Eq. (18)]).

Lemma 1.

$$\lambda^n = a_n + a_{n-1}(\lambda - b_{k-1}) + \dots + a_{n-k+1}(\lambda^{k-1} - b_{k-1}\lambda^{k-2} - \dots - b_1). \tag{14}$$

Lemma 2. *Relation* (13) *holds for integers* $x_0, x_1, \dots, x_{k-1}$ *if and only if the number*

$$x_0 + x_1(\lambda - b_{k-1}) + \dots + x_{k-1}(\lambda^{k-1} - b_{k-1}\lambda^{k-2} - \dots - b_1)$$

is invertible in $\mathbf{Z}[\lambda]$.

Note that the mapping $T : \mathbf{Q}(\lambda) \to M_k(\mathbf{Q})$ defined by

$$T(x_0 + x_1(\lambda - b_{k-1}) + \dots + x_{k-1}(\lambda^{k-1} - b_{k-1}\lambda^{k-2} - \dots - b_1)) = A(x_0, x_1, \dots, x_{k-1})$$

is an embedding of the field $\mathbf{Q}(\lambda)$ into the matrix ring $M_k(\mathbf{Q})$. In fact, for $\mu \in \mathbf{Q}(\lambda)$, the matrix $T(\mu)$ is the matrix of the operator $\hat{\mu}$, $\hat{\mu}(x) = \mu x$, in the basis $\langle 1, \lambda, \dots, \lambda^{k-1}\rangle$. In particular, $T(\lambda) = B$. Taking into account the definitions of the homomorphism T and of the polynomial F_B, one can see that

$$\det T(x_0 + x_1(\lambda - b_{k-1}) + \dots + x_{k-1}(\lambda^{k-1} - b_{k-1}\lambda^{k-2} - \dots - b_1)) = F_B(x_0, x_1, \dots, x_{k-1}).$$

Thus, Lemma 2 is a reformulation of the corollary to Lemma 2 in [3].

Theorem 1 [3]. *Consider the sequence a_n defined by relations (2)–(3). Let the polynomial f defined by (6) be irreducible over $\mathbf{Q}$ and let λ be a root of f. Define a polynomial F_B by (8), (9), and (11). Then relation (13) is characteristic for the sequence a_n if and only if*

$$(\mathbf{Z}[\lambda])^* = \{\pm\lambda^n : n \in \mathbf{Z}\}. \tag{15}$$

Remark. In [3], this result was not stated explicitly, but it was obtained as a step in the proof of the main result of [3] (see the proof of Theorem 1 in [3] and, in particular, Eq. (19)).

It follows from Theorem 1 that if relation (13) is characteristic, then the free rank of the group $(\mathbf{Z}[\lambda])^*$ does not exceed 1. Combining this statement with the Dirichlet theorem on units (see [1, Chapter II, §4, Theorem 5]), we get the following corollary.

Corollary 1. *If relation (13) is characteristic, then one of the following conditions holds:*
(1) $k = 2$;
(2) $k = 3$, *and the polynomial f has exactly one real root;*
(3) $k = 4$, *and the polynomial f has no real roots.*

Note that the conditions of Corollary 1 are not sufficient. We call a sequence *exceptional* if it satisfies one of the conditions of Corollary 1 but relation (13) is not characteristic. Examples of such sequences will be given later. In addition, in this paper we write explicitly all exceptional sequences of orders 2 and 3.

For exceptional sequences, the group $\{\pm\lambda^n : n \in \mathbf{Z}\}$ is not the whole group $(\mathbf{Z}[\lambda])^*$, but its subgroup of finite index. This allows us to amplify Eq. (13) to a characteristic system.

4. Second-order sequences

Second-order sequences have been investigated in [10, 14, 6]; see also [12, Chapter II]. We consider this case from another point of view. Furthermore, this case allows us to demonstrate the main ideas of the general scheme for a natural simple example.

First, we find the restrictions on the coefficients b_0, b_1. Let us recall that, by our assumptions, $b_0 = \pm 1$, and the polynomial

$$f(\lambda) = t^2 - b_1 t - b_0 \tag{16}$$

is irreducible over $\mathbf{Q}$. As was noted above (see Sec. 2), we exclude the case of periodic sequences with a cyclotomic polynomial f. For this reason, for second-order sequences we have to demand that f has no complex roots, i.e., the inequality

$$b_1^2 + 4b_0 \geq 0 \tag{17}$$

holds. The polynomial f is irreducible if and only if

$$b_1^2 + 4b_0 \quad \text{is not an integer square.} \tag{18}$$

Obviously, conditions (4), (17), and (18) are equivalent to the system

$$b_0 = \pm 1, \quad b_1 \neq 0, \quad b_1^2 + 4b_0 > 0.$$

Lemma 3. *Let $k = 2$, $c_0 = \pm 1$, $c_1 \in \mathbf{Z}$, $c_1 \neq 0$, $c_1^2 + 4c_0 > 0$. Let μ satisfy the equation*

$$\mu^2 - c_1\mu - c_0 = 0. \tag{19}$$

Let $\lambda = \mu^n$ or $\lambda = -\mu^n$ for some integer n. The inclusion $\mu \in \mathbf{Z}[\lambda]$ holds if and only if one of the following conditions holds:
(i) $|n| = 1$;
(ii) $|n| = 2$, $|c_1| = 1$, *and* $c_0 = 1$.

Proof. Necessity. Note that $\lambda \in \mathbf{Z}[\mu]$. Hence, for $\mu \in \mathbf{Z}[\lambda]$ we have

$$\mathbf{Z}[\mu] = \mathbf{Z}[\lambda].$$

In particular, $\langle 1, \mu \rangle$ and $\langle 1, \lambda \rangle$ are bases of the same modulus. Therefore, the discriminants of these bases are equal, $D(1, \mu) = D(1, \lambda)$ (for example, see [1, Chapter 2, §2]).

Let

$$\lambda = x\mu + y. \tag{20}$$

Then $D(1, \lambda) = x^2 D(1, \mu)$. Hence, $x = \pm 1$.

Taking the norm of λ, we have $N(\lambda) = N(x\mu + y) = x^2 N(\mu) + xy \operatorname{Tr}(\mu) + y^2 = -c_0 x^2 + c_1 xy + y^2$. On the other hand, $N(\lambda) = (N(\pm\mu^n)) = (N(\mu^n)) = (N(\mu))^n = (-c_0)^n$. Therefore,

$$-c_0 x^2 + c_1 xy + y^2 = (-c_0)^n.$$

Case 1. $c_0 = -1$. Since $x = \pm 1$, we have $c_1 xy + y^2 = 0$, i.e., either $y = 0$ or $y = -xc_1$. If $y = 0$, then $\lambda = x\mu = \pm\mu$, and $n = 1$. If $y = -xc_1$ then, by (19) and (20), $\lambda = x(\mu - c_1) = xc_0\mu^{-1} = \mp\mu^{-1}$, and $n = -1$.

Case 2. $c_0 = 1$, n is odd. Since $x = \pm 1$, we get the same relation $c_1 xy + y^2 = 0$ as above. As in case 1, we have $n = \pm 1$.

Case 3. $c_0 = 1$, n is even. Then $c_1 xy + y^2 = (-c_0)^n + c_0 x^2 = 2$. Taking into account that x, y, and c_1 are integers, one can list all their possible values (see Table 1). In addition, Table 1 contains the values of $g_\mu(t)$ (the minimal polynomial for μ over $\mathbf{Q}$) and the corresponding values of λ and n.

TABLE 1.

y	x	c_1	$g_\mu(t)$	λ	n
2	1	-1	t^2+t-1	$\mu+2=\mu^{-2}$	-2
2	-1	1	t^2-t-1	$-\mu+2=\mu^{-2}$	-2
-2	1	1	t^2-t-1	$\mu-2=-\mu^{-2}$	-2
-2	-1	-1	t^2+t-1	$-\mu-2=-\mu^{-2}$	-2
1	1	1	t^2-t-1	$\mu+1=\mu^2$	2
1	-1	-1	t^2+t-1	$-\mu+1=\mu^2$	2
-1	1	-1	t^2+t-1	$\mu-1=-\mu^2$	2
-1	-1	1	t^2-t-1	$-\mu-1=-\mu^2$	2

This completes the proof of necessity.

Sufficiency. Condition (i) is obviously sufficient, since $\mu \in (\mathbf{Z}[\mu])^*$ if $c_0 = \pm 1$. As to condition (ii), one can directly check that it is sufficient (see the values of λ in Table 1). This completes the proof.

If μ satisfies the equation $\mu^2 - \mu - 1 = 0$, then $\lambda^2 - 3\lambda + 1$ is the minimal polynomial for $\lambda = \mu^2$ and $\lambda = \mu^{-2}$, and $\lambda^2 + 3\lambda + 1$ is the minimal polynomial for $\lambda = -\mu^2$ and $\lambda = -\mu^{-2}$. We obtain the same polynomials if μ satisfies the equation $\mu^2 + \mu - 1 = 0$, and $\lambda = \pm\mu^2$, $\lambda = \pm\mu^{-2}$.

Theorem 2. *Let $k = 2$, $b_0 = \pm 1$, $b_1 \in \mathbf{Z}$, $b_1 \neq 0$, $b_1^2 + 4b_0 > 0$.*
(1) *If $b_0 = -1$, $b_1 = \pm 3$, then $[(\mathbf{Z}[\lambda])^* : \{\pm\lambda^n | n \in \mathbf{Z}\}] = 2$.*
(2) *In all the remaining cases, $(\mathbf{Z}[\lambda])^* = \{\pm\lambda^n | n \in \mathbf{Z}\}$.*

Proof. The proof is immediate by Lemma 3.

Theorem 3. *Let $k = 2$, $b_0 = \pm 1$, $b_1 \in \mathbf{Z}$, $b_1 \neq 0$, $b_1^2 + 4b_0 > 0$. Relation (3) is characteristic for sequence (2)–(3) if and only if*

$$\langle b_0, b_1 \rangle \notin \{\langle -1, 3 \rangle, \langle -1, -3 \rangle\}.$$

Proof. The proof is immediate by Theorems 1 and 2.

Remark 1. Consider the exceptional sets $\langle b_0, b_1 \rangle$ in detail.

First note that, for second-order sequences with $b_0 = -1$, more careful analysis of (12) leads to the relation

$$F_B(-a_n, -a_{n-1}) = F_B(a_n, a_{n-1}) = (\det B)^n = 1^n = 1.$$

Let $b_0 = -1$, $b_1 = 3$, and $\lambda^2 - 3\lambda + 1 = 0$. In this case,

$$F_B(x_0, x_1) = x_0^2 - 3x_0 x_1 + x_1^2.$$

One can take $\mu = \lambda - 1$ as a fundamental unit of the ring $\mathbf{Z}[\lambda]$. In addition, $\lambda = \mu^2$. By Lemma 2, all superfluous solutions of Eq. (13) correspond to numbers of the form $\pm\mu^{2n+1}$. Namely, all superfluous solutions are given by $\langle y_n, z_n \rangle$, $\langle -y_n, -z_n \rangle$, where $\mu^{2n+1} = y_n + z_n(\lambda - b_1)$. Note that $\mu^{2n+1} = \mu\lambda^n = (\lambda - 1)\lambda^n = \lambda^{n+1} - \lambda^n$. By Lemma 1,

$$\mu^{2n+1} = a_{n+1} - a_n + (a_n - a_{n-1})(\lambda - b_1),$$

i.e., $y_n = a_{n+1} - a_n$, $z_n = a_n - a_{n-1}$. Taking into account the recurrent relation (2) with $b_1 = 3$, we have $y_n = 2a_n - a_{n-1}$. A straightforward calculation shows that

$$F_B(y_n, z_n) = F_B(-y_n, -z_n) = -F_B(a_n, a_{n-1}) = -1.$$

Thus, in this case one can take the relation

$$F_B(x_0, x_1) = 1 \tag{21}$$

as a characteristic relation instead of (13).

For the same reasons, in the case $b_0 = -1$, $b_1 = -3$, one can take (21) as a characteristic relation.

Remark 2. Let $b_0 = -1$, $|b_1| \neq 3$, and $b_1^2 + 4b_0 > 0$. By Theorems 1 and 2, in this case relation (13) is characteristic, i.e., it has no superfluous solutions. But for $b_0 = -1$ we have, as in Remark 1, $F_B(-a_n, -a_{n-1}) = F_B(a_n, a_{n-1}) = 1$. Therefore, the equation

$$F_B(x_0, x_1) = -1$$

has no integer solutions. Hence, if $b_0 = -1$, then we can consider a simpler characteristic relation (21) instead of (13).

5. Third-order sequences

First, we find restrictions on the coefficients b_i. By Corollary 1 to Theorem 1, it is necessary that the cubic polynomial f defined for $k = 3$ by (6) has exactly one real root. It is well known (for example, see [8, §26]) that this condition holds if and only if the discriminant of f is negative:

$$D = b_1^2 b_2^2 + 4b_1^3 - 4b_0 b_2^3 - 27b_0^2 - 18b_0 b_1 b_2 < 0. \tag{22}$$

Exclude from these polynomials the polynomials reducible over $\mathbf{Q}$. Since $b_0 = \pm 1$, the real root of f is 1 or -1, and both its complex roots are roots of unity lying in some quadratic field (i.e., they are primitive roots of unity of degree 3, 4, or 6).

TABLE 2.

f	D
$x^3 - x^2 + x - 1 = (x^2+1)(x-1)$	-16
$x^3 + x^2 + x + 1 = (x^2+1)(x+1)$	-16
$x^3 - 1 = (x^2+x+1)(x-1)$	-27
$x^3 + 2x^2 + 2x + 1 = (x^2+x+1)(x+1)$	-3
$x^3 - 2x^2 + 2x - 1 = (x^2-x+1)(x-1)$	-3
$x^3 + 1 = (x^2-x+1)(x+1)$	-27

All reducible polynomials f with $b_0 = \pm 1$ and $D < 0$ are listed in Table 2.

Since the discriminant of an irreducible cubic polynomial is not equal to $-3, -16, -27$ (see [8, p. 126]), to exclude the case of reducibility we may impose the following restriction along with relation (22):

$$D \neq -3, -16, -27. \tag{23}$$

Later we reduce the problem of description of third-order exceptional sequences to the problem on the number of representations of 1 by a binary cubic form of negative discriminant. Exact estimates for the number of such representations were found by Delone, see [8, Chapter VI].

Theorem 4 (Delone). *Let $c_0 = \pm 1$, $D = c_1^2c_2^2 + 4c_1^3 - 4c_0c_2^3 - 27c_0^2 - 18c_0c_1c_2 < 0$, $D \neq -3, -16, -27$. Consider the equation*

$$x^3 - c_2x^2y - c_1xy^2 - c_0y^3 = 1. \tag{$*$}$$

(1) *If $D = -23$, then Eq. $(*)$ has 5 integer solutions.*
(2) *If $D = -31$ or $D = -44$, then Eq. $(*)$ has 4 integer solutions.*
(3) *In all the remaining cases, i.e., if $D < -44$, Eq. $(*)$ has at most 3 integer solutions.*

For a proof, see [8, Chapter VI].

By Theorem 1 and Corollary 1, to find all exceptional third-order sequences we have to find all units λ in cubic orders of negative discriminant for which there exists a unit $\mu \in \mathbf{Z}[\lambda]$ such that $\lambda = \pm\mu^n$, $|n| \geq 2$. Let us note that we may take $-\mu$ instead μ. Since for their norms we have $N(\mu) = -N(-\mu)$, without loss of generality we may assume that $N(\mu) = 1$, i.e., the constant term of the minimal polynomial for μ equals -1.

First consider the case $D < -44$.

Lemma 4. *Let $k = 3$, $c_0 = 1$, $D = c_1^2c_2^2 + 4c_1^3 - 4c_2^3 - 27 - 18c_1c_2 < -44$. Let μ satisfy the equation*

$$\mu^3 - c_2\mu^2 - c_1\mu - 1 = 0, \tag{24}$$

and let $\lambda = \mu^n$ or $\lambda = -\mu^n$ for some integer n. The inclusion $\mu \in \mathbf{Z}[\lambda]$ holds if and only if one of the following conditions is fulfilled:
(i) *$|n| = 1$;*
(ii) *$c_1 = 0$, $c_2 \geq 2$, and $|n| = 2$;*
(iii) *$c_2 = 0$, $c_1 \leq -2$, and $|n| = 2$.*

Proof. Necessity. Since $\lambda = \pm\mu^n \in \mathbf{Z}[\mu]$ and $\mu \in \mathbf{Z}[\lambda]$ by our hypothesis, we have

$$\mathbf{Z}[\mu] = \mathbf{Z}[\lambda].$$

In particular, $\langle 1, \mu, \mu^2 \rangle$ and $\langle 1, \lambda, \lambda^2 \rangle$ are bases of the same modulus. Let us consider, along with the first basis, the following one: $\langle 1, \zeta, \eta \rangle$, where $\zeta = \mu - c_2$ and $\eta = \mu^2 - c_2\mu - c_1$. It easy to check the following relations (let us recall here that $c_0 = 1$):

$$\begin{aligned} \mu\zeta &= \eta + c_1, \\ \zeta^2 &= c_1 - c_2\zeta + \eta, \\ \mu\eta &= 1, \\ \zeta\eta &= 1 - c_2\eta, \\ \eta^2 &= \zeta - c_1\eta. \end{aligned} \tag{25}$$

Let

$$\lambda = z + x\zeta + y\eta. \tag{26}$$

By the above relations, we have

$$\lambda^2 = z^2 + c_1x^2 + 2xy + (-c_2x^2 + y^2 + 2xz)\zeta + (x^2 - c_1y^2 + 2yz - 2c_2xy)\eta\,.$$

The transition matrix between the bases $\langle 1, \zeta, \eta\rangle$ and $\langle 1, \lambda, \lambda^2\rangle$ is

$$C(\lambda) = \begin{pmatrix} 1 & z & z^2 + c_1x^2 + 2xy \\ 0 & x & -c_2x^2 + y^2 + 2xz \\ 0 & y & x^2 - c_1y^2 + 2yz - 2c_2xy \end{pmatrix}.$$

Since the transition matrix is unimodular, i.e., it is a matrix with integer entries whose determinant is equal to ± 1 (see [1, Chapter 2, §2, Section 1]), we have

$$\det C(\lambda) = x^3 - c_2x^2y - c_1xy^2 - y^3 = \pm 1.$$

Since $\mathbf{Z}[\lambda] = \mathbf{Z}[-\lambda]$, the numbers λ and $-\lambda$ satisfy the hypotheses of our lemma simultaneously. Therefore, it is sufficient to consider one of the numbers λ and $-\lambda$. Since

$$C(-\lambda) = C(\lambda) \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

$\det C(\lambda) = -\det C(-\lambda)$. Therefore, without loss of generality we may assume that $\det C(\lambda) = 1$ and that

$$x^3 - c_2x^2y - c_1xy^2 - y^3 = 1 \tag{27}$$

(otherwise, take $-\lambda$ instead of λ).

We consider λ^{-1} similarly. Let $\lambda^{-1} = r + p\zeta + q\eta$. As above, let $C(\lambda^{-1})$ be the transition matrix between the bases $\langle 1, \zeta, \eta\rangle$ and $\langle 1, \lambda^{-1}, \lambda^{-2}\rangle$:

$$C(\lambda^{-1}) = \begin{pmatrix} 1 & r & r^2 + c_1p^2 + 2pq \\ 0 & p & -c_2p^2 + q^2 + 2pr \\ 0 & q & p^2 - c_1q^2 + 2qr - 2c_2pq \end{pmatrix}.$$

Now we prove that

$$\det C(\lambda) = -\det C(\lambda^{-1})\,.$$

Note that λ satisfies the cubic equation

$$\lambda^3 - b_2\lambda^2 - b_1\lambda - b_0 = 0\,,$$

where $b_i \in \mathbf{Z}$ and $b_0 = \pm 1$ (since λ is a unit of the ring $\mathbf{Z}[\mu]$); in particular, $b_0^{-1} = b_0$. Hence,

$$\begin{aligned} \lambda^{-1} &= b_0\lambda^2 - b_0b_2\lambda - b_0b_1, \\ \lambda^{-2} &= -b_1\lambda^2 + (b_1b_2 + b_0)\lambda + b_1^2 - b_0b_2. \end{aligned}$$

Therefore, the transition matrix between the bases $\langle 1, \lambda, \lambda^2\rangle$ and $\langle 1, \lambda^{-1}, \lambda^{-2}\rangle$ is

$$C = \begin{pmatrix} 1 & -b_0 b_1 & b_1^2 - b_0 b_2 \\ 0 & -b_0 b_2 & b_1 b_2 + b_0 \\ 0 & b_0 & -b_1 \end{pmatrix}.$$

Since $C(\lambda^{-1}) = C(\lambda) \cdot C$, we have $\det C(\lambda^{-1}) = \det C(\lambda) \det C = -b_0^2 \det C(\lambda) = -\det C(\lambda) = -1$.

Consequently,

$$p^3 - c_2 p^2 q - c_1 p q^2 - q^3 = -1. \tag{28}$$

Thus, we reduce our problem to the analysis of representations of unity by binary cubic forms.

Let us indicate other relations between x, y, z, p, q, r that we need below. Since $(z+x\zeta+y\eta)(r+p\zeta+q\eta) = \lambda\lambda^{-1} = 1$, we have, by the multiplication table (25),

$$zr + c_1 xp + xq + yp = 1, \tag{29}$$

$$zp + xr - c_2 xp + yq = 0, \tag{30}$$

$$zq + xp - c_2 xq - c_2 yp + yr - c_1 yq = 0. \tag{31}$$

By the hypotheses of our lemma, $D < -44$. Therefore, by the Delone theorem (Theorem 4), Eq. (27) has at most three integer solutions. It is easy to find two of them:

$$\begin{aligned} x &= 1, \quad y = 0; \\ x &= 0, \quad y = -1. \end{aligned} \tag{32}$$

Denote the third solution (if it exists) by (X, Y). If a pair (x, y) satisfies (27) and $x = 0$ or $y = 0$, then (x, y) is one of the two trivial solutions (32). Hence,

$$X \neq 0, \qquad Y \neq 0.$$

The solutions of Eq. (28) are $(-1, 0)$, $(0, 1)$, and (if the third solution exists) $(-X, -Y)$.

Let us consider possible combinations of the values of x, y, p, q. Note that, in general, admissible values of x, y, p, q are not independent. In fact, $c = \lambda + \lambda^{-1} \notin \mathbf{Z}$ (otherwise λ satisfies a quadratic equation with integer coefficients, which is impossible). Thus, we have to exclude the following three cases, where $x = -p$, $y = -q$:

$$\begin{aligned} x &= 1, & y &= 0, & p &= -1, & q &= 0, \\ x &= 0, & y &= -1, & p &= 0, & q &= 1, \\ x &= X, & y &= Y, & p &= -X, & q &= -Y. \end{aligned}$$

Consider the remaining six cases.

Case 1. $x = 1$, $y = 0$, $p = 0$, $q = 1$. By (31), $z = c_2$. It follows from (26) and from the definition of η and ζ that $\lambda = c_2 + \zeta = \mu$, i.e., $n = 1$ in this case.

Case 2. $x = 0$, $y = -1$, $p = -1$, $q = 0$. By (30), $z = 0$. It follows from (26) and from the definition of η and ζ that $\lambda = -\eta = -(\mu^2 - c_2\mu - c_1) = -\mu^{-1}$, i.e., $n = -1$ in this case.

We have already proved that if Eq. (27) has only two integer solutions, then any λ satisfying the hypotheses of our lemma admits only trivial values $\pm\mu$, $\pm\mu^{-1}$.

Let us consider the cases where (27) has three solutions.

Case 3. $x = 1$, $y = 0$, $p = -X$, $q = -Y$. By (31), $-zY - X + c_2 Y = 0$. In particular, $Y \mid X$. Since the pair (X, Y) satisfies (27), we conclude that $Y = \pm 1$.

(a) $Y = 1$. Substituting this into (27), we get

$$X^3 - c_2X^2 - c_1X - 1 = 1. \tag{33}$$

Therefore, $X \mid 2$, and X takes the values ± 1, ± 2. We claim that in all these cases the values of the discriminant D are not smaller than -44, i.e., they do not satisfy the hypotheses of our lemma.

If $X = 1$, then $c_1 = -1 - c_2$, by (33). Hence, $D = c_2^4 - 6c_2^3 + 7c_2^2 + 6c_2 - 31 = (c_2^2 - 3c_2 - 1)^2 - 32 \geq -32$.

If $X = -1$, then $c_1 = 3 + c_2$, by (33). Hence, $D = c_2^4 + 6c_2^3 + 27c_2^2 + 54c_2 + 81 = (c_2^2 + 3c_2 + 9)^2 \geq 0$.

If $X = 2$, then $c_1 = 3 - 2c_2$, by (33). Hence, $D = 4c_2^4 - 48c_2^3 + 189c_2^2 - 270c_2 + 81 = (2c_2^2 - 12c_2 + 45/4)^2 - 729/16$. Let us estimate $|2c_2^2 - 12c_2 + 45/4| = |2(c_2 - 3)^2 - 27/4|$. For integer c_2, the minimum of the above modulus is attained at $c_2 = 1$ or $c_2 = 5$. It equals $5/4$. Therefore, $D \geq 25/16 - 729/16 = -44$.

If $X = -2$, then $c_1 = 5 + 2c_2$, by (33). Hence, $D = 4c_2^4 + 48c_2^3 + 229c_2^2 + 510c_2 + 473 = (2c_2^2 + 12c_2 + 85/4)^2 + 343/16 > 0$. The analysis of case (a) is completed.

(b) $Y = -1$. As was noted above, $X \neq 0$. Then, by (27), X satisfies the equation

$$X^2 + c_2X - c_1 = 0. \tag{34}$$

Denote its second solution by X'. Since $(1, 0)$, $(0, -1)$, $(X, -1)$, and $(X', -1)$ satisfy (27), and by the Delone theorem, for $D < -44$, Eq. (27) has at most three solutions, we have either $X = X'$ or $X' = 0$.

Let us show that the equality $X = X'$ is impossible. If $X = X'$, then $c_2^2 + 4c_1 = 0$, by (34). Moreover, $X = -c_2/2$. Since $x = 1$, $y = 0$, $p = -X = c_2/2$, $q = -Y = 1$, we have $z = c_2/2$, by (31). Therefore, $\lambda = c_2/2 + \zeta = \mu - c_2/2$. But $\lambda^2 = \mu^2 - c_2\mu + c_2^2/4 = \mu^2 - c_2\mu - c_1 = \mu^{-1}$, which contradicts the hypothesis $\lambda = \pm\mu^n$, where n is an integer.

Let us consider the case $X' = 0$. Then $c_1 = 0$ by (34). Since $X \neq 0$, we have $X = -c_2$. First, we find the admissible values of c_2. Since $c_1 = 0$, we have $D = -4c_2^3 - 27$ and, by the hypothesis, $D < -44$, $c_2 \geq 2$. Finally, we find n. Since $x = 1$, $y = 0$, $p = -X = c_2$, and $q = -Y = 1$, we deduce from (31) that $z = 0$. Therefore, $\lambda = \zeta = \mu - c_2$. Since $c_1 = 0$, we have $\mu^2\lambda = \mu^2(\mu - c_2) = 1$ and $\lambda = \mu^{-2}$, i.e., $n = -2$.

The analysis of case 3 is completed.

Case 4. $x = 0$, $y = -1$, $p = -X$, $q = -Y$. By (30), $-zX - Y = 0$. In particular, $X \mid Y$. Since the pair (X, Y) satisfies (27), we conclude that $X = \pm 1$.

(a) $X = -1$. Substituting this in (27), we obtain

$$-1 - c_2Y + c_1Y^2 - Y^3 = 1. \tag{35}$$

Therefore, $Y \mid 2$, and Y takes the values ± 1, ± 2. As in case 3(a), we claim that $D \geq -44$, i.e., the hypotheses of our lemma are not satisfied.

If $Y = -1$, then $c_2 = 1 - c_1$, by (35) . Hence, $D = c_1^4 + 6c_1^3 + 7c_1^2 - 6c_1 - 31 = (c_1^2 + 3c_1 - 1)^2 - 32 \geq -32$.

If $Y = 1$, then $c_2 = -3 + c_1$, by (35). Hence, $D = c_1^4 - 6c_1^3 + 27c_1^2 - 54c_1 + 81 = (c_1^2 - 3c_1 + 9)^2 \geq 0$.

If $Y = -2$, then $c_2 = -3 - 2c_1$, by (35). Hence, $D = 4c_1^4 + 48c_1^3 + 189c_1^2 + 270c_1 + 81 = (2c_1^2 + 12c_1 + 45/4)^2 - 729/16$. As above, for integer c_1, the minimum of $|2c_1^2 + 12c_1 + 45/4| = |2(c_1 + 3)^2 - 27/4|$ is attained at $c_1 = -1$ or $c_1 = -5$. It is equal to $5/4$. Therefore, $D \geq 25/16 - 729/16 = -44$.

If $Y = 2$, then $c_2 = -5 + 2c_1$, by (35). Hence, $D = 4c_1^4 - 48c_1^3 + 229c_1^2 - 510c_1 + 473 = (2c_1^2 - 12c_1 + 85/4)^2 + 343/16 > 0$. The analysis of case (a) is completed.

(b) $X = 1$. As was noted above, $Y \neq 0$. Then, by (27), Y satisfies the equation

$$Y^2 + c_1Y + c_2 = 0. \tag{36}$$

Denote its second solution by Y' (Y' is also an integer). Since $(1, 0)$, $(0, -1)$, $(1, Y)$, and $(1, Y')$ satisfy (27), and by the Delone theorem, for $D < -44$, Eq. (27) has at most three solutions, we conclude that either $Y = Y'$ or $Y' = 0$.

Let us show that the equality $Y = Y'$ is impossible. If $Y = Y'$, then $c_1^2 - 4c_2 = 0$ by (36). In addition, $Y = -c_1/2$. Since $x = 0$, $y = -1$, $p = -X = -1$, and $q = -Y = c_1/2$, we have $z = -c_1/2$ by (30). Therefore,

$\lambda = -c_1/2 - \eta = -\mu^2 + c_2\mu + c_1/2 = -\mu^{-1} - c_1/2$. But $\lambda^2 = \mu^{-2} + c_1\mu^{-1} + c_1^2/4 = \mu^{-2} + c_1\mu^{-1} + c_2 = \mu^1$, which contradicts the hypothesis $\lambda = \pm\mu^n$, where n is an integer. Hence, $Y \neq Y'$.

Let us consider the case $Y' = 0$. Then $c_2 = 0$ by (36). Since $Y \neq 0$, we have $Y = -c_1$. First, we find the admissible values of c_1. Since $c_2 = 0$, we have $D = 4c_1^3 - 27$ and, by the hypothesis $D < -44$, $c_1 \leq -2$. Finally, we find n. Since $x = 0$, $y = -1$, $p = -X = -1$, $q = -Y = c_1$, we deduce from (30) that $z = -c_1$. Therefore, $\lambda = -c_1 - \eta = -\mu^2$ (recall that $c_2 = 0$), i.e., $n = 2$. The analysis of case 4 is completed.

Case 5. $x = X, y = Y, p = -1, q = 0$. Analysis similar to that in case 3 (one should consider $-\lambda^{-1} = -r + \zeta$ instead of λ) shows that $c_1 = 0$, $c_2 \geq 2$, $|n| = 2$.

Case 6. $x = X, y = Y, p = 0, q = 1$. Analysis similar to that in case 4 (one should consider $-\lambda^{-1} = -r - \eta$, instead of λ) shows that $c_1 \leq -2$, $c_2 = 0$, $|n| = 2$.

This completes the proof of necessity.

Sufficiency. The proof is straightforward.

Now we consider the case of small $|D|$. The scheme is the same as in Lemma 4. Let us note that it is sufficient to take a fundamental unit (say, ε) of the corresponding ring and to find all λ such that $\lambda = \pm\varepsilon^n$, $|n| \geq 2$, and $\mathbf{Z}[\lambda] = \mathbf{Z}[\varepsilon]$.

The minimal polynomials of fundamental units of cubic orders with discriminants -23, -31, and -44 are listed in Table 3. These fundamental units are taken from [8, p. 230]. (In fact, in [8] their inverses are given.)

TABLE 3.

-23	$\varepsilon^3 - \varepsilon - 1$
-31	$\varepsilon^3 - \varepsilon^2 - 1$
-44	$\varepsilon^3 - \varepsilon^2 - \varepsilon - 1$

Lemma 5. (1) *Assume that $D = -23$. Let ε satisfy the equation $\varepsilon^3 - \varepsilon - 1 = 0$ and let $\lambda = \varepsilon^n$ or $\lambda = -\varepsilon^n$ for some integer n. The inclusion $\varepsilon \in \mathbf{Z}[\lambda]$ holds if and only if $n \in \{\pm1, \pm2, \pm3, \pm4, \pm5, \pm9\}$.*

(2) *Assume that $D = -31$. Let ε satisfy the equation $\varepsilon^3 - \varepsilon^2 - 1 = 0$ and let $\lambda = \varepsilon^n$ or $\lambda = -\varepsilon^n$ for some integer n. The inclusion $\varepsilon \in \mathbf{Z}[\lambda]$ holds if and only if $n \in \{\pm1, \pm2, \pm3, \pm5\}$.*

(3) *Assume that $D = -44$. Let ε satisfy the equation $\varepsilon^3 - \varepsilon^2 - \varepsilon - 1 = 0$ and let $\lambda = \varepsilon^n$ or $\lambda = -\varepsilon^n$ for some integer n. The inclusion $\varepsilon \in \mathbf{Z}[\lambda]$ holds if and only if $n \in \{\pm1, \pm3\}$.*

Proof. Necessity. Let $D = -23$. As in the proof of Lemma 4, we reduce the problem to determination of units $\lambda = z + x\varepsilon + y(\varepsilon^2 - 1)$ such that

$$x^3 - xy^2 - y^3 = 1.$$

All solutions of this equation are the following pairs (see [8, Chapter VI, p. 317]):

$$\langle 1, 0\rangle, \quad \langle 0, -1\rangle, \quad \langle 1, -1\rangle, \quad \langle -1, -1\rangle, \quad \langle 4, 3\rangle.$$

Since λ is a unit in $\mathbf{Z}[\varepsilon]$, its norm equals ±1, i.e.,

$$N(z + x\varepsilon + y(\varepsilon^2 - 1)) = \det\begin{pmatrix} z - y & y & x \\ x & z & x + y \\ y & x & z \end{pmatrix} = \pm1.$$

Substituting the admissible values of x and y, we obtain cubic equations in the variable z. All solutions with integer z, the corresponding values of λ, and $g_\lambda(t)$ (the minimal polynomials for λ) are listed in Table 4. (We refer to these values below.)

TABLE 4.

z	x	y	λ	$g_\lambda(t)$
0	1	0	ε	t^3-t-1
-1	1	0	ε^{-4}	t^3+3t^2+2t-1
1	1	0	ε^3	t^3-3t^2+2t-1
1	0	-1	ε^{-5}	t^3-4t^2+5t-1
-1	0	-1	$-\varepsilon^2$	t^3+2t^2+t+1
0	0	-1	$-\varepsilon^{-1}$	t^3-t^2+1
0	1	-1	ε^{-2}	t^3-t^2+2t-1
-1	1	-1	$-\varepsilon^3$	t^3+2t^2+3t+1
-2	-1	-1	$-\varepsilon^5$	t^3+5t^2+4t+1
-1	-1	-1	$-\varepsilon^4$	t^3+2t^2-3t+1
2	-1	-1	$-\varepsilon^{-9}$	$t^3-7t^2+12t+1$
5	4	3	ε^9	t^3-12t^2-7t-1

Let $D=-31$. Similarly, we reduce the problem to determination of units $\lambda = z + x(\varepsilon-1)+y(\varepsilon^2-\varepsilon)$ such that

$$x^3-x^2y-y^3=1.$$

All integer solutions of this equation are the following pairs (see [8, Chapter VI, p. 317]):

$$\langle 1,0\rangle,\quad \langle 0,-1\rangle,\quad \langle -1,-1\rangle,\quad \langle 3,2\rangle.$$

Since λ is a unit in $\mathbf{Z}[\varepsilon]$, we have

$$N(z+x(\varepsilon-1)+y(\varepsilon^2-\varepsilon)) = \det\begin{pmatrix} -x+z & y & x \\ x-y & -x+z & y \\ y & x & z \end{pmatrix} = \pm 1.$$

As above, substituting the admissible values of x and y, we find z. All the solutions are listed in Table 5.

TABLE 5.

z	x	y	λ	$g_\lambda(t)$
0	1	0	ε^{-2}	t^3+2t^2+t-1
1	1	0	ε	t^3-t^2-1
1	0	-1	ε^{-3}	t^3-3t^2+4t-1
0	0	-1	$-\varepsilon^{-1}$	t^3+t+1
-2	-1	-1	$-\varepsilon^3$	t^3+4t^2+3t+1
-1	-1	-1	$-\varepsilon^{-2}$	t^3-2t^2+t+1
1	-1	-1	$-\varepsilon^{-5}$	t^3-5t^2+6t+1
4	3	2	ε^5	t^3-6t^2-5t-1

Let $D=-44$. Similarly, we reduce the problem to determination of units $\lambda = z+x(\varepsilon-1)+y(\varepsilon^2-\varepsilon-1)$ such that

$$x^3-x^2y-xy^2-y^3=1.$$

All integer solutions of this equation are the following pairs (see [8, Chapter VI, p. 317]):

$$\langle 1,0\rangle,\quad \langle 0,-1\rangle,\quad \langle 2,1\rangle,\quad \langle -103,-56\rangle.$$

Since λ is a unit in $\mathbf{Z}[\varepsilon]$, we have

$$\det\begin{pmatrix} -x-y+z & y & x \\ x-y & -x+z & x+y \\ y & x & z \end{pmatrix} = \pm 1.$$

Substituting the admissible values of x and y, we find z. All the solutions are listed in Table 6.

TABLE 6.

z	x	y	λ	$g_\lambda(t)$
1	1	0	ε	t^3-t^2-t-1
-1	1	0	$-\varepsilon^{-3}$	t^3+5t^2+7t+1
0	0	-1	$-\varepsilon^{-1}$	t^3-t^2+t+1
4	2	1	ε^3	t^3-7t^2+5t-1

This completes the proof of necessity.

Sufficiency. One can directly check that, for all values of n listed in our lemma, the discriminant of order $\mathbf{Z}[\pm\lambda]$ is equal to the discriminant of maximal order (i.e., it is equal to -23, -31, and -44, respectively). Therefore, $\mathbf{Z}[\pm\lambda]$ coincides with the maximal order of the corresponding field, and $\varepsilon \in \mathbf{Z}[\pm\lambda]$. This completes the proof.

Theorem 5. *Let λ satisfy the equation $\lambda^3 - b_2\lambda^2 - b_1\lambda - b_0 = 0$, where $b_0 = \pm 1$, $D = b_1^2 b_2^2 + 4b_1^3 - 4b_0 b_2^3 - 27b_0^2 - 18b_0 b_1 b_2 < 0$, $D \neq -3, -16, -27$.*

(1) *If $\langle b_0, b_1, b_2\rangle$ is one of the triples*

$$\begin{array}{llll} \langle 1,-2,1\rangle, & \langle 1,-1,2\rangle, & \langle -1,-2,-1\rangle, & \langle -1,-1,-2\rangle, \\ \langle 1,2,1\rangle, & \langle 1,-1,-2\rangle, & \langle -1,2,-1\rangle, & \langle -1,-1,2\rangle, \\ \langle 1,2t,t^2\rangle, & \langle 1,-t^2,-2t\rangle, & \langle -1,2t,-t^2\rangle, & \langle -1,-t^2,2t\rangle, \end{array}$$

where $t \geq 2$, then $[(\mathbf{Z}[\lambda])^* : \{\pm\lambda^n \mid n \in \mathbf{Z}\}] = 2$.

(2) *If $\langle b_0, b_1, b_2\rangle$ is one of the triples*

$$\begin{array}{llll} \langle 1,-2,3\rangle, & \langle 1,-3,2\rangle, & \langle -1,-2,-3\rangle, & \langle -1,-3,-2\rangle, \\ \langle 1,-3,4\rangle, & \langle 1,-4,3\rangle, & \langle -1,-3,-4\rangle, & \langle -1,-4,-3\rangle, \\ \langle 1,-5,7\rangle, & \langle 1,-7,5\rangle, & \langle -1,-5,-7\rangle, & \langle -1,-7,-5\rangle, \end{array}$$

then $[(\mathbf{Z}[\lambda])^* : \{\pm\lambda^n \mid n \in \mathbf{Z}\}] = 3$.

(3) *If $\langle b_0, b_1, b_2\rangle$ is one of the triples*

$$\langle 1,3,2\rangle, \quad \langle 1,-2,-3\rangle, \quad \langle -1,3,-2\rangle, \quad \langle -1,-2,3\rangle,$$

then $[(\mathbf{Z}[\lambda])^* : \{\pm\lambda^n \mid n \in \mathbf{Z}\}] = 4$.

(4) *If $\langle b_0, b_1, b_2\rangle$ is one of the triples*

$$\begin{array}{llll} \langle 1,5,6\rangle, & \langle 1,-6,-5\rangle, & \langle -1,5,-6\rangle, & \langle -1,-6,5\rangle, \\ \langle 1,-4,5\rangle, & \langle 1,-5,4\rangle, & \langle -1,-4,-5\rangle, & \langle -1,-5-4\rangle, \end{array}$$

then $[(\mathbf{Z}[\lambda])^* : \{\pm\lambda^n \mid n \in \mathbf{Z}\}] = 5$.

(5) *If* $\langle b_0, b_1, b_2\rangle$ *is one of the triples*

$$\langle 1,7,12\rangle, \quad \langle 1,-12,-7\rangle, \quad \langle -1,7,-12\rangle, \quad \langle -1,-12,7\rangle,$$

then $[(\mathbf{Z}[\lambda])^* : \{\pm\lambda^n \mid n \in \mathbf{Z}\}] = 9$.

(6) *In all the remaining cases,* $(\mathbf{Z}[\lambda])^* = \{\pm\lambda^n \mid n \in \mathbf{Z}\}$.

Proof. All the triples $\langle b_0, b_1, b_2\rangle$ listed in items (1)–(5) are coefficients of the minimal polynomials for units λ such that $\lambda = \pm\mu^n$, $|n| \geq 2$, and $\mu \in \mathbf{Z}[\lambda]$ (see Lemmas 4 and 5). Computation of indices of the corresponding subgroups is straightforward.

Theorem 6. *Let* $k = 3$ *and let the sequence* a_n *be defined by* (2)–(3). *Let* $D = b_1^2b_2^2 + 4b_1^3 - 4b_0b_2^3 - 27b_0^2 - 18b_0b_1b_2 < 0$, $D \neq -3, -16, -27$. *Relation* (13) *is characteristic for the sequence* a_n *if and only if the triple* $\langle b_0, b_1, b_2\rangle$ *is not listed in items* (1)–(5) *of Theorem* 5.

Proof. This follows immediately from Theorems 1 and 5.

Now we can construct $\mathbf{Z}$-Diophantine representations of the sets of values of third-order sequences.

For $k = 3$ and fixed coefficients b_0, b_1, b_2 of the recurrent relation, define the sets

$$\mathcal{M}(b_0, b_1, b_2) = \{\langle y_0, y_1, y_2\rangle : \exists n \in \mathbf{Z}\ [y_i = a_{n-i},\ i = 0,1,2]\} \tag{37}$$

and

$$\mathcal{M}^+(b_0, b_1, b_2) = \{\langle y_0, y_1, y_2\rangle : \exists n \in \mathbf{N}\ [y_i = a_{n-i},\ i = 0,1,2]\}. \tag{38}$$

Theorem 7. *Let* b_0, b_1, b_2 *be the same as in Theorem* 5. *Let the sequence* $a_n = a_n(b_0, b_1, b_2)$ *be defined by* (2)–(3) *and let the sets* $\mathcal{M}$ *and* $\mathcal{M}^+$ *be defined by* (37), (38).

(1) $\langle y_0, y_1, y_2\rangle \in \mathcal{M}(b_0, b_1, b_2)$ *if and only if there exist integers* x_0, x_1, x_2 *such that* (13) *holds and*

$$\bigvee_{i=1}^{360} \{A(y_0, y_1, y_2) = B^i(A(x_0, x_1, x_2))^{360}\}, \tag{39}$$

where the matrices B *and* $A(x_0, x_1, x_2)$ *are defined by* (8) *and* (9), *respectively.*

(2) $\langle y_0, y_1, y_2\rangle \in \mathcal{M}^+(b_0, b_1, b_2)$ *if and only if there exist integers* x_0, x_1, x_2 *such that* (13) *and* (39) *hold, and*

$$\det((A^2(y_0, y_1, y_2) - E)(B^2 - E)) > 0. \tag{40}$$

Proof. Take the same λ as in Theorem 5. Let $\xi \in (\mathbf{Z}[\lambda])^*$. We first prove that $\xi = \lambda^n$ for some integer n if and only if there exist $\mu \in (\mathbf{Z}[\lambda])^*$ and $i \in \{1, 2, \ldots, 360\}$ such that

$$\xi = \lambda^i\mu^{360}. \tag{41}$$

Let such i and μ exist. By Theorem 5, the index of the subgroup $\langle\lambda^n \mid n \in \mathbf{Z}\rangle$ in the group $(\mathbf{Z}[\lambda])^*$ divides 360. Hence, $\mu^{360} \in \{\lambda^n \mid n \in \mathbf{Z}\}$ and $\xi \in \{\lambda^n \mid n \in \mathbf{Z}\}$. Conversely, if $\xi = \lambda^n$, then it is sufficient to take $i \equiv n \pmod{360}$, $1 \leq i \leq 360$, and $\mu = \lambda^{\frac{n-i}{360}}$.

Write $\xi = y_0 + y_1(\lambda - b_2) + y_2(\lambda^2 - b_2\lambda - b_1)$ and $\mu = x_0 + x_1(\lambda - b_2) + x_2(\lambda^2 - b_2\lambda - b_1)$. Applying the monomorphism T defined in Sec. 3 to relation (41), we prove the first claim.

To prove the second claim, note that λ is an eigenvalue of the matrix B and $\xi = y_0 + y_1(\lambda - b_2) + y_2(\lambda^2 - b_2\lambda - b_1)$ is an eigenvalue of the matrix $A(y_0, y_1, y_2)$. Moreover, each of these matrices has exactly one real eigenvalue. By the first assertion, conditions (39) and (40) hold if and only if $\xi = \lambda^n$ for some integer n. Condition (40) means that real eigenvalues of the matrices $A(y_0, y_1, y_2)$ and B either both lie inside the interval $(-1, 1)$ or both lie outside the interval $[-1, 1]$. This is equivalent to the fact that $n > 0$. This completes the proof.

Remark. If we restrict ourselves to sequences for which relation (13) is characteristic, we can find simpler Diophantine representations of the sets $\mathcal{M}(b_0, b_1, b_2)$ and $\mathcal{M}^+(b_0, b_1, b_2)$. Indeed, since $[(\mathbf{Z}[\lambda])^* : \{\lambda^n \,|\, n \in \mathbf{Z}\}] = [\{\pm\lambda^n \,|\, n \in \mathbf{Z}\} : \{\lambda^n \,|\, n \in \mathbf{Z}\}] = 2$ in this case, one can replace the constant 360 by 2 in Theorem 7. On the other hand, the above formulation included all possible cases.

This research was supported in part by the ISSEP, grants a96-1965 and a97-2261.

Translated by M. A. Vsemirnov.

REFERENCES

1. Z. I. Borevich and I. R. Shafarevich, *Theory of Numbers* [in Russian], Moscow (1972).
2. M. A. Vsemirnov, "On Diophantine representations of linear recurrent sequences," in: *II International Conference: Algebraic, Probabilistic, Geometric, Combinatorial, and Functional Methods in Number Theory. Abstracts* [in Russian], Voronezh (1995), p. 36.
3. M. A. Vsemirnov, "Diophantine representations of linear recurrent sequences. I," *Zap. Nauchn. Semin. POMI*, **227**, 52–60 (1995).
4. M. A. Vsemirnov, "Direct constructions of Diophantine representations of linear recurrent sequences," in: *Materials of International Conference and Chebyshev's Readings, Dedicated to the 175th Anniversary of P. L. Chebyshev's Birth* [in Russian], Moscow, **1** (1996), pp. 101–103.
5. M. A. Vsemirnov, "Diophantine representations of linear recurrent sequences of small orders," in: *Number Theory Conference, Abstracts*, Eger (1996), pp. 40–41.
6. M. Davis, "An explicit Diophantine definition of the exponential function," *Comm. Pure Appl. Math.*, **24**, 137–145 (1971).
7. M. Davis, H. Putnam, and J. Robinson, "The decision problem for exponential Diophantine equations," *Ann. Math.*, **74**, 425–436 (1961).
8. B. N. Delone and D. K. Faddeev, "Theory of irrationalities of third degree," *Trudy Mat. Inst. Akad. Nauk SSSR*, **11** (1940).
9. P. Kiss, "On some properties of linear recurrences," *Publ. Math.*, **30**, 273–281 (1983).
10. N. K. Kossovskii, "Diophantine representation of the sequence of solutions of the Pell equation," *Zap. Nauchn. Semin. LOMI*, **20**, 49–59 (1971).
11. Yu. V. Matiyasevich, "Enumerable sets are Diophantine," *Dokl. Akad. Nauk SSSR*, **191**, 278–282 (1970).
12. Yu. V. Matiyasevich, *Hilbert's Tenth Problem* [in Russian], Moscow (1993).
13. Yu. V. Matiyasevich (Yu. V. Matijasevič) and J. Robinson, "Reduction of an arbitrary Diophantine equation to one in 13 unknowns," *Acta Arithmetica*, **27**, 521–553 (1975).
14. G.V. Chudnovskii, "Diophantine predicates," *Usp. Mat. Nauk*, **25**, 185–186 (1970).