Introduction

Linear recurring sequences have a wide range of application from the field of solving diophantine equations, through rational approximation and random number generation to cryptology. The present work deals with the different aspects of linear recurring sequences and related topics. However the mainstream of our studies is the examination of uniform distribution of sequences and application of the obtained results in constructing efficient pseudo-random number generators and sequences with general distribution.

The properties of the linear recurring sequences have been investigated by several authors from different points of view.

The periodicity of recurring sequences reduced modulo m was studied in the thirties by Ward. He in [49] could prove that if u is a third-order linear recurring sequence and m_1, m_2 are relatively prime positive integers both greater than 1, then the period length of the sequence reduced modulo $m_1 m_2$ is the least common multiple of the period lengths of the same sequence reduced modulo m_1 and m_2. He also proved that u is purely periodic modulo $m_1 m_2$ if and only if it is purely periodic both modulo m_1 and m_2. Furthermore, he proved some properties of the period length, too.

In [50] he obtained results on the number of appearances of the residue classes of a third-order linear recurring sequence.

Duparc in [13] and [14] investigated the period length of general linear recurring sequences reduced to finite residue classes over unique factorization domains.

Bundschuh and Shiue in [5] generalized the result of Bundschuh [4] and gave a sufficient condition on the uniform distribution of general second-order linear recurring sequences reduced modulo prime powers.

Niederreiter in [29] proved that the Fibonacci sequence is uniformly distributed modulo m if and only if $m = 5^s$.

Nathanson [28] gave a criterion for the uniform distribution of a second-order linear recurring sequence modulo primes.

Webb and Long in [51] characterized the general second-order linear recurring sequences to be uniformly distributed reduced modulo prime powers and Bumby [3] with respect to general moduli.

Niederreiter and Shiue in [31] and [32] gave necessary and sufficient condition for a linear recurring sequence of order less than 5 to be uniformly distributed over finite fields. Here they proved that a general linear recurring sequence could be uniformly distributed over a finite field only if its characteristic polynomial had a multiple root over the same field. This leads to the observation, that over the integers, a linear recurring sequence can be uniformly distributed modulo p (and thus modulo p^s) only if p divides the discriminant of its characteristic polynomial. They also gave

here a sufficient condition for the characteristic polynomial of recurrence sequences over prime fields, such that if this simple condition holds, then the corresponding sequence is uniformly distributed. This result lets us construct pseudo random sequences with good distribution properties and a large period length.

Narkiewicz [27] gave an overview of the uniform distribution of linear recurring sequences and among others, he studied the uniform distribution of second-order linear recurring sequences in general residue class systems.

Turnwald in [46] and [47] gave a complete characterization of second and third-order linear recurring sequences defined over Dedekind domains to be uniformly distributed in residue class systems with finite norm.

Tichy and Turnwald [45] applied the previous result and gave a criterion for uniform distribution of third-order linear recurring sequences over the integers.

Drmota and Tichy in [10] gave a survey of the topic and proved uniform distribution and weak uniform distribution properties of several sorts of recurring sequences.

Carlip and Jacobson in [6] studied a more general distribution property of linear recurring sequences and gave a criterion for this stability property for second-order linear recurring sequences modulo powers of 2.

Uniform distribution of general sequences are studied in [23] where the concept of completely uniformly distributed sequences are also developed.

As a standard monograph on non uniform random number generation we refer to Devroye [8]. One can find there various algorithms for generating random number sequences with different distributions. See also Winkler [52].

Furthermore, we mention Knuth's fundamental book [22], where different notions of pseudo-randomness are considered.

It should be remarked, that pseudo-random sequences are used in various applications, especially in Monte Carlo methods for solving different kinds of problems, such as numerical integration, optimization, simulation of stochastic processes etc. For a survey on random number generation and Quasi-Monte Carlo methods we refer to Niederreiter [30].

Another theory we will use in the present work is the field of linear transformations.

Linear transformations have a great importance in applied sciences. The most well-known and most frequently used are the Fourier transform and the Laplace transformation.

A particular linear transformation which is also often used for different purposes is the so-called Walsh transformation. For example, in digital picture processing it can be used as filtering transformation (see e.g. in the book of Yaroslavsky [53]). In a more special application in character recognition it is used as symmetry representation of digitalized images (cf. [18]).

As an application of linear recurring sequences we will prove some divisibility properties of lacunary polynomials, namely trinomials. As general works in this subject we refer to Rédei [37], Nagell [25] and Schinzel [40], [41] and [42].

The structure of the present thesis is the following:

In **Chapter 1** we give the most general definitions and results we use in the later parts.

In **Chapter 2** we prove some general properties of Dedekind-domains paying particular attention to residue systems generated by ideals with finite norm. We should mention, that the results here and in Chapter 3 are the generalization of [19], where the case of rational integers were investigated.

Chapter 3 is built around the problem of uniform distribution of linear recurring sequences. Here we study among others the periodicity and the hereditary of periodicity of sequences in residue class systems modulo powers of prime ideals. The observations lead to the main result Theorem 3.36 of the chapter:
For every linear recurring sequence in a Dedekind-domain we can find an integer S depending only on the degree of the recurrence relation, such that if the sequence is uniformly distributed modulo P^S, where P is a prime ideal with finite norm, then the sequence is uniformly distributed modulo every power of the ideal P.

In **Chapter 4** we give a method for constructing linear recurring sequences of integers, such that the sequence is uniformly distributed modulo every power of 2. With the use of these sequences we can develop pseudo-random number generators with very good properties. In **Appendix A** we give an example of such a linear recurring sequence of order 9943.

In **Chapter 5** we provide a method to create pseudo-random number sequences with Gaussian distribution using linear transformations of uniformly distributed sequences. The method we present is based on the Berry-Esséen Theorem and on the existence of very well uniformly distributed sequences. In **Appendix A** we present some experimental results related to this chapter, where we analyze different pseudo-random number sequences after linear transformations. The results here are mainly from the paper [20].

Finally in **Chapter 6** we use linear recurring sequences for proving a kind of finiteness of trinomials having quadratic divisors. The chapter covers the results of [21].

Chapter 1

Basic definitions and results

Dedekind-domains are defined in several ways in the literature. We will give the one which is the most suitable for our purposes.

Definition 1.1. *Let R be an integral domain. We call R a* **Dedekind-domain**, *if for every ideal I of R we can find prime ideals $P_1, \ldots, P_k$ unique up to ordering, such that $I = P_1 \cdot \ldots \cdot P_k$.*

For general properties of Dedekind-domains see [7], [15], [16], [26], [35] and [48].

Definition 1.2. *Let R be a Dedekind-domain and let $I \subseteq R$ be an ideal. We will call the cardinality of the ring R/I the* **norm** *of I and we will denote it by $N(I)$.*

Remark 1.3. *Let I and J be two relatively prime ideals of R, e.g. let $I + J = R$. Suppose further that I and J have both finite norm. Then*

$$N(I \cdot J) = N(I) \cdot N(J) \ .$$

The proof of the above statement is based on the Chinese Remainder Theory. (See e.g. in [26].*)*

The same can be proven for arbitrary I and J as a consequence of Corollary 2.2.

Definition 1.4. *Let R be a Dedekind-domain and let $a_0, \ldots, a_{d-1} \in R$ and*

$$u = \{u_n\}_{n=0}^{\infty}$$

be a sequence in R satisfying the **recurrence relation**

$$u_{n+d} = a_{d-1}u_{n+d-1} + \cdots + a_0 u_n \quad \textit{for} \quad n = 0, 1, \ldots \quad .$$

Then u is called a **linear recurring sequence** *(for short* **l.r.s.***) with* **defining coefficients** *$a_0, \ldots, a_{d-1}$ and* **initial values** *$u_0, \ldots, u_{d-1}$.*

The integer d is called the **order** *of the recurrence and the polynomial*

$$P(x) = x^d - a_{d-1}x^{d-1} - \cdots - a_0$$

is called a **characteristic polynomial** *of u.*

Remark 1.5. *It is easy to see that a linear recurring sequence satisfies several recurrence relations. In particular, one can say that if $P(x) \in R[x]$ is a characteristic polynomial of a recurring sequence, then $P(x) \cdot Q(x)$ is also a characteristic polynomial of the sequence for all $Q(x) \in R[x]$. (See e.g.* [46].*)*

Remark 1.6. *By the previous remark, the order of a linear recurring sequence is not definite. However, since the different values of the orders of a sequence are positive numbers, there exists a unique smallest.*

Definition 1.7. *Let $d(u)$ be the smallest integer for which there exists a recurrence relation of order $d(u)$ for the sequence u. This number is said to be the* **minimal order** *of the recurring sequence and a corresponding characteristic polynomial is said to be a* **minimal characteristic polynomial** *of u.*

Remark 1.8. *As we will see in Lemma 3.7, the minimal characteristic polynomial of a linear recurring sequence is also unique.*

Definition 1.9. *Let R be a Dedekind-domain, $m \in R$ and let $P \subseteq R$ be a prime ideal. We will denote by $\nu_P(m) \in \mathbb{N}$ the* **P-adic valuation** *of m, which is defined by the following:*

$$(m) \subseteq P^{\nu_P(m)} \qquad but \qquad (m) \setminus P^{\nu_P(m)+1} \neq \emptyset \ ,$$

where (m) denotes **the ideal generated by** *m.*

Definition 1.10. *Let u be a sequence in the Dedekind-domain R and let $I \subseteq R$ be an ideal. We say that u is* **periodic** *modulo I with* **period length** *$\varrho \in \mathbb{N}$, if there exists $\varrho_0 \in \mathbb{N}$, such that*

$$u_{n+\varrho} \equiv u_n \mod I \quad for\ all \quad n \geq \varrho_0 \ .$$

The smallest $\varrho_0 = \varrho_{0,I}(u)$ and $\varrho = \varrho_I(u)$ with the previous property will be called the **preperiod** *and* **minimal period length** *of u modulo I respectively.*

If $\varrho_{0,I}(u) = 0$ then u is said to be **purely periodic** *modulo m.*

Remark 1.11. *Let R be a Dedekind-domain, let u be a linear recurring sequence in R and let $I \subseteq R$ be an ideal with finite norm. A simple observation shows that u is periodic modulo I.*

Definition 1.12. *Let u be a sequence in the Dedekind-domain R and let $I \subseteq R$ be an ideal with finite norm. We will say that u is* **uniformly distributed** *(for short u.d.) modulo I if*

$$\lim_{N\to\infty} \frac{1}{N} \#\left\{n \leq N | u_n \equiv a \mod I\right\} = \frac{1}{N(I)}$$

for all $a \in R$.

Remark 1.13. *Let R be a Dedekind-domain, let u be a linear recurring sequence in R and let $I, J \subseteq R$ be two ideals with finite norm, such that $I \subseteq J$. One can prove that if u is u.d. modulo I, then it is u.d. modulo J. The proof is based on the fact that if $a_1, \ldots, a_{N(I)}$ is a complete residue system modulo I, then the cardinality of the set*

$$\{a' \mid a' \in \{a_1, \ldots, a_{N(I)}\} \quad and \quad a' \equiv a \mod J\}$$

with some $a \in R$, is independent of the value of a.

Definition 1.14. *Let u be a l.r.s. in the Dedekind-domain R, defined by the coefficients $a_0, \dots, a_{d-1}$ with initial values $u_0, \dots, u_{d-1}$ and let $P \subseteq R$ be a prime ideal. Let*

$$\bar{u}_n(k) = (u_{n+k-1}, u_{n+k-2}, \dots, u_n)^{tr}$$

*denote the nth k-***dimensional state vector** *and*

$$M(u) = \begin{pmatrix} a_{d-1} & a_{d-2} & \dots & a_1 & a_0 \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 \end{pmatrix}$$

the **companion matrix** *of u.*

Remark 1.15. *With the above notations we have*

$$\bar{u}_n(d) = M(u)^n \bar{u}_0(d) \ ,$$

which will be used frequently in the paper.

Remark 1.16. *We mention that if we reduce a linear recurring sequence modulo some ideal in a Dedekind-domain, then we get a linear recurring sequence in the residue class system, which may have different properties than the original sequence (e.g. the minimal order of the reduced sequence may became smaller).*

By Remark 1.16 it has sense to introduce the following notations:

Definition 1.17. *Let s be a positive integer. With the notation of Definition 1.14 $d_P(u,s)$ will denote* **the minimal order**, *$\varrho_P(u,s)$ the* **minimal period length**, *$M_P(u,s)$ the* **companion matrix** *and $a_{s,0}, \dots, a_{s,d_P(u,s)-1}$ the* **defining coefficients corresponding to the minimal recurrence relation** *of u modulo P^s.*

Remark 1.18. *As far as there is no confusion, we will simplify our notation by omitting unnecessary parameters, for instance, by cancelling the sign of the ideal P.*

For further properties of linear recurring sequences we refer to [24].

Chapter 2

Dedekind-domains and modules

For the discussions of the later chapters we will need some special properties of Dedekind-domains. In this chapter we state all the results we will use. The material of this and the 4th chapter is a generalization of [19].

Throughout the chapter let R be a Dedekind-domain, and let P be a prime ideal of R. Suppose that R/P has $N(P)$ elements, and $N(P) < \infty$. Since R is a Dedekind-domain, P is maximal and R/P is a (finite) field (see e.g. [16]). Hence, we know that $N(P) = \pi^l$ with some rational prime π and an integer $l \geq 1$ (see e.g. [24]). First we turn to the determination of $N(P^k)$. For this we need the following:

Theorem 2.1. *Let $k \in \mathbb{N}$. Then the additive groups of the rings R/P and P^{k-1}/P^k are isomorphic.*

Proof. See e.g. [26]. □

Corollary 2.2. *Let $k \in \mathbb{N}$. Then $N(P^k) = N(P)^k$.*

Proof. By the isomorphism theorem of groups, we know that the additive groups of $(R/P^k)/(P^{k-1}/P^k)$ and R/P^{k-1} are isomorphic, thus

$$N(P^k) = \#\{P^{k-1}/P^k\}N(P^{k-1}) = N(P)N(P^{k-1}) \ .$$

Hence, by induction, we obtain the statement. □

In general Dedekind-domains we cannot ensure that if some elements are in the same ideal of the ring, they have common non-unit divisor. Fortunately, since we will work in residue class systems, some more general results will be enough for the cancellation of 'common factors'.

Theorem 2.3. *Let $k, s \in \mathbb{N}$, $P \subseteq R$ be a prime ideal and let $p \in P^k \setminus P^{k+1}$. Then for every $q \in P^k$ there exists $r \in R$, such that $p \cdot r \equiv q \mod P^s$. In particular, if $q \in P^k \setminus P^{k+1}$, then $r \in R \setminus P$.*

Proof. If $s \leq k$, then $p \equiv q \equiv 0 \mod P^s$, thus $r = 1$ is suitable.

Suppose now that $s > k$. Let $r_1, \ldots, r_n \in R$ be a complete residue system modulo P^{s-k}, where by Corollary 2.2 we find $n = N(P)^{s-k}$. If $1 \leq i, j \leq n$, such that $i \neq j$, then

$$r_i \not\equiv r_j \mod P^{s-k} \ ,$$

which is equivalent to

$$r_i - r_j \notin P^{s-k} \ . \tag{2.1}$$

Since $p \notin P^{k+1}$, relation (2.1) holds if and only if

$$p(r_i - r_j) \notin P^k P^{s-k} = P^s \ ,$$

i.e.

$$pr_i \not\equiv pr_j \mod P^s \ .$$

This yields that $pr_1, \ldots, pr_n$ represent n different residue classes modulo P^s.

Let $q_1, \ldots, q_m \in R$ be a complete residue system modulo P^k, such that $q_1 = 0$. Clearly $m = N(P)^k$.

We claim that $pr_i + q_j$ with $1 \le i \le n$ and $1 \le j \le m$ is a complete residue system modulo P^s. To prove this, we have to show that all the residue classes $pr_i + q_j$ are different, since $n \cdot m = N(P)^s$. But $pr_i + q_j \equiv pr_{i'} + q_{j'} \mod P^s$ implies that $pr_i + q_j \equiv pr_{i'} + q_{j'} \mod P^k$, i.e. $q_j \equiv q_{j'} \mod P^k$. This means that $j = j'$, whence $pr_i \equiv pr_{i'} \mod P^s$ i.e. $i = i'$.

By the above claim, there exist $1 \le i_0 \le n$ and $1 \le j_0 \le m$, such that

$$q \equiv pr_{i_0} + q_{j_0} \mod P^s \ .$$

Hence

$$q - pr_{i_0} \equiv q_{j_0} \mod P^s \ ,$$

and thus

$$0 \equiv q - pr_{i_0} \equiv q_{j_0} \mod P^k \ .$$

This yields that $j_0 = 1$ i.e. $q_{j_0} = 0$, whence

$$q \equiv pr_{i_0} \mod P^s \ .$$

Setting $r = r_{i_0}$ we obtain the first part of the theorem. The second statement is clear if we notice that $q \notin P^{k+1}$ implies $pr \notin P^{k+1}$, whence $r \notin P$. □

Corollary 2.4. *Let $s \in \mathbb{N}$, $P \subseteq R$ be a prime ideal and let $p \in R \setminus P$. Then there exists $r \in R \setminus P$, such that $p \cdot r \equiv 1 \mod P^s$.*

Proof. If we fix $k = 0$ and $q = 1$ in Theorem 2.3, we obtain the result. □

Corollary 2.5. *Let $r, k, s \in \mathbb{N}$ and $\lambda_1, \ldots, \lambda_r \in R$, such that*

$$P^{k+1} + (\lambda_1) + \cdots + (\lambda_r) = P^k$$

(e.g. k will be the highest exponent of P, such that P^k is a divisor of all the ideals $\lambda_1, \ldots, \lambda_r$) and let $p \in P^k \setminus P^{k+1}$. Then there exist $\lambda'_1, \ldots, \lambda'_r \in R$ and $i \in \{1, \ldots, r\}$, such that

$$\lambda_j \equiv p\lambda'_j \mod P^s$$

for $j = 1 \ldots r$ and $\lambda'_i \notin P$.

Proof. The condition

$$P^{k+1} + (\lambda_1) + \cdots + (\lambda_r) = P^k$$

yields that $(\lambda_1), \ldots, (\lambda_r)$ are divisible by P^k, but at least one of them – say (λ_i) – is not divisible by P^{k+1}. Then $\lambda_1, \ldots, \lambda_r \in P^k$, but $\lambda_i \notin P^{k+1}$. Hence, substituting q by λ_j and r by λ'_j in Theorem 2.3, the property $\lambda'_i \notin P$ is deduced from the last sentence of the theorem. □

Corollary 2.6. *Let $r, k, s \in \mathbb{N}$ and $\lambda_1, \ldots, \lambda_r \in R$, such that*

$$(\lambda_1) + \cdots + (\lambda_r) \subseteq P^k$$

and let $p \in P^k \setminus P^{k+1}$. Then there exist $\lambda'_1, \ldots, \lambda'_r \in R$ and $i \in \{1, \ldots, r\}$, such that

$$\lambda_j \equiv p\lambda'_j \mod P^s$$

for $j = 1 \ldots r$.

Proof. Since $P^{k+1} + (p) = P^k$, we have

$$P^{k+1} + (p) + (\lambda_1) + \cdots + (\lambda_r) = P^k \ .$$

By the previous corollary, there exist $\lambda'_0, \lambda'_1, \ldots, \lambda'_r \in R$, such that

$$\lambda_j \equiv p\lambda'_j \mod P^s$$

for $j = 1 \ldots r$. □

Definition 2.7.

Let R be a Dedekind-domain and let d be a positive integer. $V(R, d)$ will denote the free module of rank d over R, which can be regarded as the Cartesian product R^d with the natural extension of addition and componentwise multiplication by elements of R. If there are no confusion, we will omit R and d.

We will say, that two vectors $a, b \in V(R, d)$ are congruent $\mod I$, if they are congruent component-wise $\mod I$.

Let $s, r \in \mathbb{N}$. The set of vectors $\{b_1, \ldots, b_r\} = B \subset V(R, d)$ is called **semi-independent** $\mod P^s$ *if*

$$\lambda_1 b_1 + \cdots + \lambda_r b_r \equiv 0 \mod P^s$$

implies that $\lambda_i \equiv 0 \mod P$ for $i = 1, \ldots, r$. Otherwise it is called **strongly dependent**.

Let $b_1, \ldots, b_r, b \in V(R, d)$. The vector b is called a **linear semi-combination** *of the elements $b_1, \ldots, b_r \mod P^s$ if $b \equiv 0 \mod P^s$ or there exist $k \in \mathbb{N}$, $p \in P^k \setminus P^{k+1}$ and $\lambda_1, \ldots, \lambda_r \in R$, such that*

$$0 \not\equiv pb \equiv \lambda_1 b_1 + \cdots + \lambda_r b_r \mod P^s$$

and $\lambda_i \not\equiv 0 \mod P$ for some $i \in \{1, \ldots, r\}$ provided that $k > 0$.

If $\{b_1, \ldots, b_r\} = B \subset V(R, d)$ is semi-independent and for all $b \in V(R, d)$, b is a semi-combination of $b_1, \ldots, b_r \mod P^s$, then B is called a **semi-basis** *of $V(R, d) \mod P^s$.*

We keep the notion of independence, combination and basis for the usual sense definition.

For arbitrary modules we usually cannot generalize all the results of linear algebra, however in our special case we can prove some important ones:

Theorem 2.8. *For every $d, s \in \mathbb{N}$ there exists a basis (in the usual sense) of $V(R,d) \mod P^s$ and it has exactly d elements.*

Proof. See e.g. Th. 7.12. (p104) of [2]. □

Further in the chapter we fix R and d, and we will use the notation V instead of $V(R,d)$.

Theorem 2.9. *Let $b_1, \ldots, b_r \in V$ be linearly dependent over R, then they are strongly dependent $\mod P^s$, for any s.*

Proof. Let $s \in \mathbb{N}$, $\lambda_1, \ldots, \lambda_r \in R$ such that

$$\lambda_1 b_1 + \cdots + \lambda_r b_r = 0 \ ,$$

and let $k \in \mathbb{N}$, such that

$$P^{k+1} + (\lambda_1) + \cdots + (\lambda_r) = P^k$$

and $p \in P^k \setminus P^{k+1}$. Then by Corollary 2.5 there exist $\lambda'_1, \ldots, \lambda'_r \in R$ and $i \in \{1, \ldots, r\}$, such that $\lambda'_i \notin P$ and $\lambda_j \equiv p\lambda'_j \mod P^{s+k}$. Thus

$$p\lambda'_1 b_1 + \cdots + p\lambda'_r b_r \equiv 0 \mod P^{s+k} \ ,$$

whence

$$\lambda'_1 b_1 + \cdots + \lambda'_r b_r \equiv 0 \mod P^s \ .$$

Hence by definition, $b_1, \ldots, b_r$ are strongly dependent $\mod P^s$. □

Theorem 2.10. *Let $b_1, \ldots, b_d \in V$ be linearly independent over R, then for any*

$$s > \nu_P(\det(b_1, \ldots, b_d)) \tag{2.2}$$

the vectors $b_1, \ldots, b_d$ are semi-independent $\mod P^s$.

Proof. Let $\lambda_1, \ldots, \lambda_d \in R$, such that

$$\lambda_1 b_1 + \cdots + \lambda_d b_d \equiv 0 \mod P^s \ .$$

This yields that

$$b = \lambda_1 b_1 + \cdots + \lambda_d b_d \in P^s \ .$$

If $b = 0$, then by the independence of $b_1, \ldots, b_d$, we have

$$\lambda_1 = \cdots = \lambda_d = 0 \ .$$

Suppose, that $b \neq 0$. Since $b_1, \ldots, b_d$ are linearly independent over R, we find

$$\det(b_1, \ldots, b_d) \neq 0 \ ,$$

and Cramer's rule can be applied. Hence

$$\lambda_i \det(b_1, \ldots, b_d) = \det(b_1, \ldots, b_d | b_i \leftarrow b) \ ,$$

for $i = 1, \ldots, d$.

Let $b = (\beta_1, \ldots, \beta_d)$. Since

$$b \equiv 0 \mod P^s ,$$

thus

$$\beta_i \equiv 0 \mod P^s$$

for $i = 1, \ldots, d$. Hence

$$\det(b_1, \ldots, b_d | b_i = p^s b) \in P^s .$$

By (2.2), we get $\det(b_1, \ldots, b_d) \notin P^s$, whence $\lambda_i \in P$ for all $i = 1, \ldots, d$. By definition this yields that $b_1, \ldots, b_d$ are semi independent $\mod P^s$. □

Remark 2.11. *If the number of independent vectors in Theorem 2.10 is less than d, there still exists a lower bound on s with the same properties.*

Corollary 2.12. *Let $b_1, \ldots, b_d \in V$ and $t = \nu_P(\det(b_1, \ldots, b_d))$. If $b_1, \ldots, b_d$ is not a semi-basis $\mod P^{t+1}$, then it is not a semi-basis $\mod P^s$ for any $s \in \mathbb{N}$, either.*

Proof. If $b_1, \ldots, b_d$ is not a semi-basis modulo P^{t+1}, then it is strongly dependent. By Theorem 2.10, this means that $b_1, \ldots, b_d$ is linearly dependent over R. Then by Theorem 2.9, we obtain the statement. □

Theorem 2.13. *If $b_1, \ldots, b_r \in V$ are semi-independent $\mod P^s$, then $r \leq d$.*

Proof. By Theorem 2.9, $b_1, \ldots, b_r$ are independent over R and thus independent over $\mathbb{Q}_R$, the quotient field of R (using the natural embedding). □

Theorem 2.14. *If $b_1, \ldots, b_d \in V(R, d)$ are semi-independent $\mod P^s$, then the set $b_1, \ldots, b_d$ is a semi-basis $\mod P^s$.*

Proof. Similarly as in the proof of Theorem 2.13, the set $b_1, \ldots, b_d$ is a basis of $V(\mathbb{Q}_R, d)$. Thus for every $b \in V(R, d)$ there exist

$$\lambda_0, \lambda_1, \ldots, \lambda_d \in R$$

, such that

$$\lambda_0 b = \lambda_1 b_1 + \cdots + \lambda_d b_d .$$

Suppose that

$$(\lambda_0) + (\lambda_1) + \cdots + (\lambda_d) + P^{k+1} = P^k$$

with some integer k and suppose that $\lambda_i \in P^k \setminus P^{k+1}$ for some $i \in \{0, \ldots, d\}$. By Corollary 2.5 there exist $\lambda'_0, \lambda'_1, \ldots, \lambda'_d \in R$, such that

$$\lambda_j \equiv \lambda'_j \lambda_i \mod P^{s+k} .$$

Then

$$\lambda_i \lambda'_0 b \equiv \lambda_i \lambda'_1 b_1 + \cdots + \lambda_i \lambda'_d b_d \mod P^{s+k} ,$$

whence

$$\lambda'_0 b \equiv \lambda'_1 b_1 + \cdots + \lambda'_d b_d \mod P^s \tag{2.3}$$

and $\lambda'_i = 1$.

Now let $b \not\equiv 0 \mod P^s$. If $\lambda'_0 b \equiv 0 \mod P^s$ held, then $i \neq 0$, and thus $b_1, \ldots, b_d$ would be strongly dependent $\mod P^s$, contrary to the assumption. Hence, $\lambda'_0 b \not\equiv 0 \mod P^s$ and by definition b is a semi-combination of $b_1, \ldots, b_d$. □

Remark 2.15. *Let $s < s'$ and suppose that $b_1, \ldots, b_d \in V$ is a semi-basis* $\bmod P^s$. *This $b_1, \ldots, b_d$ is also a semi-basis* $\bmod P^{s'}$, *otherwise it would be strongly dependent* $\bmod P^{s'}$, *which would yield*

$$\lambda_1 b_1 + \cdots + \lambda_d b_d \equiv 0 \mod P^{s'}$$

for some $\lambda_1, \ldots, \lambda_d$ not all in P. But then the same holds $\bmod P^s$ *which would contradict the semi-independence of $b_1, \ldots, b_d$.*

However, more can be proved:

Theorem 2.16. *Let $s \leq s'$ and suppose that $b_1, \ldots, b_d \in V$ is a semi-basis* $\bmod P^s$. *If $b \in V$, then there exist $\lambda_1, \ldots, \lambda_d \in R$ and $p \in P^{s-1}$ such that*

$$pb \equiv \lambda_1 b_1 + \cdots + \lambda_d b_d \mod P^{s'} .$$

Proof. Extending the proof of Theorem 2.14, the congruence (2.3) implies

$$\lambda'_0 b \equiv \lambda'_1 b_1 + \cdots + \lambda'_d b_d \mod P^{s'} , \tag{2.4}$$

where by (2.3), we find that $\nu_P(\lambda'_0) \leq s-1$. If we multiply both sides of (2.4) by some $q \in P^{s-1-\nu_P(\lambda'_0)}$, then – setting $p = q \cdot \lambda'_0$ – we obtain the theorem. □

Chapter 3

Results on recurring sequences

In this chapter we collected results on linear recurring sequences. We focused on the uniform distribution of the sequences in residue class systems. For this we examined the change of periodicity and other related properties when we change the residue class system by extension.

The following lemmas about polynomials are useful for the later analysis of the characteristic polynomials of linear recurring sequences.

Lemma 3.1. *Let $k, n \in \mathbb{N}$, R be a Dedekind-domain, $P \subseteq R$ be a prime ideal and let $Q, Q_1, Q_2 \in R[x]$.*

Suppose that

$$Q = Q_1 \cdot Q_2 \ ,$$
$$Q_1 \in P^n[x] \setminus P^{n+1}[x]$$
and
$$Q_2 \in P^k[x] \setminus P^{k+1}[x] \ .$$

Then

$$Q \in P^{n+k}[x] \setminus P^{n+k+1}[x] \ .$$

Proof. Let

$$Q_1 = a_l x^l + \cdots + a_0 \ ,$$
$$Q_2 = b_m x^m + \cdots + b_0$$
and
$$Q = c_{m+l} x^{m+l} + \cdots + c_0 \ .$$

Then we have

$$c_h = a_h b_0 + a_{h-1} b_1 + \cdots + a_0 b_h \ ,$$

where $0 \leq h \leq m + l$. Since

$$a_0, \ldots, a_h \in P^n \quad \text{and} \quad b_0, \ldots, b_h \in P^k \ ,$$

thus

$$a_h b_0, \ldots, a_0 b_h \in P^{n+k} \ ,$$

whence

$$c_h \in P^{n+k} \quad \text{for all} \quad 0 \leq h \leq m + l \ ,$$

i.e. $Q \in P^{n+k}[x]$. (The coefficients which are not explicitly defined, are assumed to be zero.)

Furthermore, since $Q_1 \notin P^{n+1}[x]$, there exists $0 \le i \le l$, such that

$$a_i \notin P^{n+1} \ ,$$

but

$$a_{i'} \in P^{n+1} \quad \text{for all} \quad 0 \le i' < i \ .$$

Similarly, there exists $0 \le j \le m$, such that

$$b_j \notin P^{k+1} \ ,$$

but

$$b_{j'} \in P^{k+1} \quad \text{for all} \quad 0 \le j' < j \ .$$

Then

$$c_{i+j} = a_{i+j}b_0 + \cdots + a_{i+1}b_{j-1} + a_ib_j + a_{i-1}b_{j+1} + \cdots + a_0b_{i+j} \ .$$

Since

$$a_0, \ldots, a_{i-1} \in P^{n+1} \quad \text{and} \quad b_0, \ldots, b_{j-1} \in P^{k+1} \ ,$$

thus

$$a_{i+j}b_0, \ldots, a_{i+1}b_{j-1}, a_{i-1}b_{j+1}, \ldots, a_0b_{i+j} \in P^{n+k+1} \ .$$

If $c_{i+j} \in P^{n+k+1}$, then $a_ib_j \in P^{n+k+1}$, but since P is a prime ideal, this contradicts the definition of i and j, whereby $c_{i+j} \notin P^{n+k+1}$ i.e. $Q \notin P^{n+k+1}[x]$. $\square$

Lemma 3.2 (Gauss-lemma). *Let R be a Dedekind-domain with quotient field $\mathbb{Q}_R$ and let $Q \in R[x]$, $Q_1, Q_2 \in \mathbb{Q}_R[x]$ be monic polynomials.*

With these assumptions $\quad Q = Q_1 \cdot Q_2 \quad$ *implies* $\quad Q_1, Q_2 \in R[x]$.

Proof. Let $p, q \in R$, such that $pQ_1, qQ_2 \in R[x]$ and suppose that the decomposition of (p) and (q) into prime ideals are

$$(p) = \prod_{i=1}^{k} P_i^{\alpha_i} \quad \text{and} \quad (q) = \prod_{i=1}^{k} P_i^{\beta_i} \ .$$

Now we can write $pqQ = pQ_1 \cdot qQ_2$.

Fix an index $1 \le i \le k$, arbitrarily. Since $Q \in R[x]$ is monic, thus

$$pqQ \in P_i^{\alpha_i+\beta_i}[x] \setminus P_i^{\alpha_i+\beta_i+1}[x] \ . \tag{3.1}$$

The leading coefficients of pQ_1 and qQ_2 are p and q respectively, thus

$$pQ_1 \notin P_i^{\alpha_i+1}[x] \quad \text{and} \quad qQ_2 \notin P_i^{\beta_i+1}[x] \ .$$

Suppose that

$$pQ_1 \in P_i^{\alpha_i'}[x] \setminus P_i^{\alpha_i'+1}[x] \quad \text{and} \quad qQ_2 \in P_i^{\beta_i'}[x] \setminus P_i^{\beta_i'+1}[x]$$

with some $\alpha_i', \beta_i' \in \mathbb{N}$. By Lemma 3.1 and (3.1),

$$\alpha_i' + \beta_i' = \alpha_i + \beta_i$$

and since

$$\alpha_i' \leq \alpha_i \quad \text{and} \quad \beta_i' \leq \beta_i \ ,$$

thus

$$\alpha_i' = \alpha_i \quad \text{and} \quad \beta_i' = \beta_i \ .$$

This yields that

$$pQ_1 \in P_i^{\alpha_i}[x] \quad \text{and} \quad qQ_2 \in P_i^{\beta_i}[x]$$

for all $1 \leq i \leq k$, whence, using that P_i are prime ideals, we get

$$pQ_1 \in \left(\prod_{i=1}^{k} P_i^{\alpha_i}\right)[x] = pR[x] \quad \text{and} \quad qQ_2 \in \left(\prod_{i=1}^{k} P_i^{\beta_i}\right)[x] = qR[x] \ .$$

Hence $Q_1, Q_2 \in R[x]$. □

Corollary 3.3. *Let R be a Dedekind-domain and let $\mathbb{Q}_R$ be its quotient field. The monic polynomial $Q \in R[x]$ is irreducible over R if and only if it is irreducible over $\mathbb{Q}_R$.*

Proof. If Q is irreducible over $\mathbb{Q}_R$ then it is obviously irreducible over R, too.

If Q is reducible over $\mathbb{Q}_R$, then there exist monic polynomials $Q_1, Q_2 \in \mathbb{Q}_R[x]$ with positive degree, such that $Q = Q_1 \cdot Q_2$. By Lemma 3.2, $Q_1, Q_2 \in R[x]$ and the statement follows. □

Remark 3.4. *If Q is not monic, then Lemma 3.2 and Corollary 3.3 do not hold. We give a counter-example.*

Let $R = \mathbb{Z}[1+\sqrt{-5}]$ and $\mathbb{Q}_R = \mathbb{Q}(1+\sqrt{-5})$. Then the polynomial $2x^2+2x+3$ is reducible over $\mathbb{Q}(1+\sqrt{-5})$ with irreducible factors

$$x + \frac{1+\sqrt{-5}}{2} \quad \textit{and} \quad 2x + 1 - \sqrt{-5} \ ,$$

but since 2 is irreducible in $\mathbb{Z}(1+\sqrt{-5})$, thus the polynomial $2x^2+2x+3$ is also irreducible over $\mathbb{Z}[1+\sqrt{-5}]$.

Lemma 3.5. *Let R be a Dedekind-domain and $Q_1, Q_2 \in R[x]$ be monic polynomials. Then there exist* $\gcd(Q_1, Q_2)$ *and* $\operatorname{lcm}(Q_1, Q_2)$.

Proof. Since $Q_1, Q_2 \in \mathbb{Q}_R[x]$, there exists the monic polynomial $\gcd(Q_1, Q_2)$ over $\mathbb{Q}_R$. Further,

$$\gcd(Q_1, Q_2) \mid Q_1$$

thus by Lemma 3.2, $\gcd(Q_1, Q_2) \in R[x]$.

Let $Q_3, Q_4 \in R[x]$, such that

$$Q_1 = \gcd(Q_1, Q_2) \cdot Q_3 \quad \text{and} \quad Q_2 = \gcd(Q_1, Q_2) \cdot Q_4 \ .$$

Then $\gcd(Q_1, Q_2) \cdot Q_3 \cdot Q_4 = \operatorname{lcm}(Q_1, Q_2) \in R[x]$. □

Lemma 3.6. *Let F be a field and u be a l.r.s. over F. Then there exists a unique minimal characteristic polynomial of u. Further, this minimal characteristic polynomial is a divisor of all the characteristic polynomials of the sequence.*

Proof. The existence and uniqueness of the minimal polynomial is proven on p.33 of [43] for number fields. The statement of the lemma is proven in Theorem 6.42 of [24] for finite fields, but the proof can be used for general fields without change. □

Lemma 3.7. *Let R be a Dedekind-domain and let u be a l.r.s. over R. Then there exists a unique minimal characteristic polynomial of u.*

Proof. Let Q be a characteristic polynomial of u over R. Since u is a l.r.s. over $\mathbb{Q}_R$, by Lemma 3.6there exists a unique minimal characteristic polynomial Q' of u over $\mathbb{Q}_R$. Since Q and Q' are monic and $Q' \mid Q$, by Lemma 3.2$Q' \in R[x]$. □

Lemma 3.8. *Let $a, b \in R$ and let u and v be two linear recurring sequences over R with characteristic polynomials Q_u and Q_v respectively. Then $au + bv$ is also a linear recurring sequence with characteristic polynomial* $\operatorname{lcm}(Q_u, Q_v)$.

Proof. Since the polynomial $\operatorname{lcm}(Q_u, Q_v)$ is divisible by both Q_u and Q_v, by Remark 1.5 $\operatorname{lcm}(Q_u, Q_v)$ is a characteristic polynomial for both sequences u and v. If two sequences both satisfy a linear recurrence relation, then any linear combination of them satisfies the same recurrence relation, whence $\operatorname{lcm}(Q_u, Q_v)$ is a characteristic polynomial for all linear combinations u and v. □

Remark 3.9. *If we define the sequence v by $v_n = u_{n+k}$ for some $k \geq 0$, then $Q_v = Q_u$ and thus Q_u is a characteristic polynomial of $au + bv$.*

Remark 3.10. *Throughout the chapter if we don't state otherwise, we suppose, that the linear recurring sequences are purely periodic in the considered residue class systems, i.e.*

$$u_{n+\varrho(u,s)} \equiv u_n \mod P^s \quad \textit{for all} \quad n = 0, 1, 2, \ldots$$

and the sequence has no preperiod.

Remark 3.11. *If $M(u)$ and $M(v)$ are the companion matrices of Q_u and Q_v respectively, then $M(u) * M(v)$ denotes the companion matrix corresponding to* $\operatorname{lcm}(Q_u, Q_v)$.

In the following lemmas we prove some properties of the minimal order of the mod P^s reduced linear recurring sequences. We will also see that the minimal order of the sequence is the best bound for the minimal order of the reduced sequences.

Lemma 3.12. *Let $\mathbb{F}$ be a finite field and let u be a l.r.s. in $\mathbb{F}$ with characteristic polynomial $Q \in \mathbb{F}[x]$. Then Q is the minimal characteristic polynomial of u if and only if the state vectors $\bar{u}_0, \ldots, \bar{u}_{d-1} \in V(\mathbb{F}, d)$ are linearly independent over $\mathbb{F}$, where d is the degree of Q.*

Proof. See e.g. Th. 6.51 of [24]. □

Lemma 3.13. *Let R be a Dedekind-domain, $P \subseteq R$ be a prime ideal with finite norm, $s \in \mathbb{N}$ and let u be a l.r.s. over R. Using the notation $d = d(u,s)$, the d dimensional state vectors $\bar{u}_0(d), \ldots, \bar{u}_{d-1}(d) \in V(R,d)$ form a semi-basis modulo P^s.*

Proof. If $s = 1$, then R/P^s is a finite field and the independence – and the semi-independence, which is the same in this case – follows from Lemma 3.12.

We will use the notation $\bar{u}_n = \bar{u}_n(d)$.

Let $s > 1$. Suppose that $\bar{u}_0, \ldots, \bar{u}_{d-1}$ is not a semi-basis modulo P^s, whence by Theorem 2.14, they are strongly dependent. This yields that there exists a set of coefficients $\lambda_0, \ldots, \lambda_{d-1} \in R$ and $k \in \{0, \ldots, d-1\}$, such that $\lambda_k \notin P$ and

$$\lambda_0 \bar{u}_0 + \cdots + \lambda_{d-1} \bar{u}_{d-1} \equiv 0 \mod P^s \ . \tag{3.2}$$

We claim that we may choose $\lambda_0, \ldots, \lambda_{d-1}$, such that

$$\lambda_{d-1} \equiv 1 \mod P^s \ .$$

Let $k = d-1$. By Corollary 2.4, there exists $\lambda \in R$ with the property

$$\lambda \cdot \lambda_{d-1} \equiv 1 \mod P^s \ .$$

Multiplying (3.2) by λ we obtain the claim for this case.

Now, suppose that $\lambda_{d-1} \in P$ for every system of $\lambda_0, \ldots, \lambda_{d-1} \in R$ which satisfies (3.2) and fix a set of coefficients $\lambda_0, \ldots, \lambda_{d-1} \in R$ satisfying (3.2), such that the corresponding k is maximal. For this k we have $k < d-1$.

Multiplying (3.2) by the companion matrix $M(u,s)$, we get

$$\begin{aligned} 0 &\equiv M(u,s)\,(\lambda_0 \bar{u}_0 + \cdots + \lambda_{d-1} \bar{u}_{d-1}) \\ &\equiv \lambda_0 M(u,s) \bar{u}_0 + \cdots + \lambda_{d-1} M(u,s) \bar{u}_{d-1} \\ &\equiv \lambda_0 \bar{u}_1 + \cdots + \lambda_{d-1} \bar{u}_d \mod P^s \ . \end{aligned} \tag{3.3}$$

By the definition of d there exist $a_{s,0}, \ldots, a_{s,d-1}$, such that

$$a_{s,0} \bar{u}_0 + \cdots + a_{s,d-1} \bar{u}_{d-1} \equiv \bar{u}_d \mod P^s \ .$$

Substituting this into (3.3), we obtain

$$\begin{aligned} 0 \equiv & \lambda_0 \bar{u}_1 + \cdots + \lambda_{d-2} \bar{u}_{d-1} \\ & + a_{s,0} \lambda_{d-1} \bar{u}_0 + \cdots + a_{s,d-1} \lambda_{d-1} \bar{u}_{d-1} \mod P^s \ . \end{aligned}$$

Set

$$\lambda'_0 = a_{s,0} \lambda_{d-1}$$

and

$$\lambda'_i = \lambda_{i-1} + a_{s,i} \lambda_{d-1} \quad \text{for} \quad i = 1, \ldots, d-1 \ .$$

Since $\lambda_{d-1} \in P$, we have $\lambda'_{k+1} \notin P$. By (3.3), $\lambda'_0, \ldots, \lambda'_{d-1}$ is also a suitable choice for the coefficients to combine 0, which contradicts the selection of k. Hence, there exists a set of coefficients $\lambda_0, \ldots, \lambda_{d-1} \in R$ satisfying (3.2), such that $u_{d-1} \notin P$, whence the claim is proven.

Choose $\lambda_0, \ldots, \lambda_{d-1} \in R$ satisfying (3.2), such that $\lambda_{d-1} \equiv 1 \mod P^s$. Hence

$$-\lambda_0 \bar{u}_0 - \cdots - \lambda_{d-2} \bar{u}_{d-2} \equiv \bar{u}_{d-1} \mod P^s \ .$$

Multiplying both sides of the congruence by $(M(u,s))^n$ we obtain

$$-\lambda_0 \bar{u}_n - \cdots - \lambda_{d-2} \bar{u}_{n+d-2} \equiv \bar{u}_{n+d-1} \mod P^s \ ,$$

which contradicts the minimal property of d. $\square$

Lemma 3.14. *Let R be a Dedekind-domain, $P \subseteq R$ be a prime ideal with finite norm, let u be a l.r.s. over R and let $r, q, s \in \mathbb{N}$, such that $0 < r \leq q$.*

If

$$\bar{u}_0(q), \ldots, \bar{u}_{r-1}(q) \in V(R, q)$$

are semi-independent modulo P^s, then

$$r \leq d(u, s) \ .$$

Proof. We will use the notation

$$d = d(u, s) \ .$$

Contrary to the lemma, suppose that $d < r$. By the definition of d there exist $\lambda_0, \ldots, \lambda_{d-1} \in R$, such that

$$\bar{u}_d(q) \equiv \lambda_0 \bar{u}_0(q) + \cdots + \lambda_{d-1} \bar{u}_{d-1}(q) \mod P^s \ ,$$

which means that $\bar{u}_0(q), \ldots, \bar{u}_{r-1}(q)$ are strongly dependent. □

Remark 3.15. *Since the minimal recurrence relation of the original sequence is also a recurrence relation for the reduced sequence, we have*

$$d(u, s) \leq d(u)$$

and since the minimal recurrence relation of the sequence reduced modulo P^{s+1} is also a recurrence relation for the same sequence reduced modulo P^s, we have

$$d(u, s) \leq d(u, s+1) \quad \textit{for all} \quad s \in \mathbb{N} \ .$$

Thus there exists an integer T, such that

$$d(u, T) = d(u, s) \quad \textit{for all} \quad s \geq T \ .$$

The smallest such a T will be denoted by $T(u)$.

Lemma 3.16. *Let R be a Dedekind-domain, u be a l.r.s. over R and let $q \geq d(u)$. Then the vectors $\bar{u}_0(q), \ldots, \bar{u}_{d(u)-1}(q)$ are independent over R.*

Proof. Let Q be the minimal characteristic polynomial of u over R.

By Lemma 3.7, the polynomial Q exists and it is also a minimal characteristic polynomial of u over $\mathbb{Q}_R$.

Let M be the q dimensional companion matrix of the sequence u corresponding to Q, which yields

$$\bar{u}_{n+1}(q) = M \bar{u}_n(q) \ .$$

Suppose that $\bar{u}_0(q), \ldots, \bar{u}_{d(u)-1}(q)$ are dependent over R. This means that there exist coefficients $\lambda_0, \ldots, \lambda_{d(u)-1} \in R$, such that

$$\lambda_0 \bar{u}_0(q) + \cdots + \lambda_{d(u)-1} \bar{u}_{d(u)-1}(q) = 0 \ .$$

Let $0 \le k \le d(u)-1$ be the largest index with the property $\lambda_k \neq 0$. For this k we can write

$$-\frac{\lambda_0}{\lambda_k}\bar{u}_0(q) - \cdots - \frac{\lambda_{k-1}}{\lambda_k}\bar{u}_{k-1}(q) = \bar{u}_k(q) \ .$$

Multiplying this equation by M^n, we obtain

$$\begin{aligned}
\bar{u}_{k+n}(q) =& M^n \bar{u}_k(q) \\
=& M^n \left(-\frac{\lambda_0}{\lambda_k}\bar{u}_0(q) - \cdots - \frac{\lambda_{k-1}}{\lambda_k}\bar{u}_{k-1}(q) \right) \\
=& -\frac{\lambda_0}{\lambda_k} M^n \bar{u}_0(q) - \cdots - \frac{\lambda_{k-1}}{\lambda_k} M^n \bar{u}_{k-1}(q) \\
=& -\frac{\lambda_0}{\lambda_k}\bar{u}_n(q) - \cdots - \frac{\lambda_{k-1}}{\lambda_k}\bar{u}_{n+k-1}(q)
\end{aligned}$$

for all $n \ge 0$. But then

$$P' = x^k + \frac{\lambda_{k-1}}{\lambda_k}x^{k-1} + \cdots + \frac{\lambda_0}{\lambda_k}$$

is also a characteristic polynomial of u over $\mathbb{Q}_R$, with degree less than $d(u)$. This is a contradiction, thus $\bar{u}_0(q), \ldots, \bar{u}_{d(u)-1}(q)$ are independent over R. □

Lemma 3.17. *Let R be a Dedekind-domain, $P \subseteq R$ be a prime ideal with finite norm and let u be a l.r.s. over R. Then*

$$d(u) = d(u, T(u)) \ .$$

Proof. Clearly,

$$d(u) \ge d(u, T(u)) \ .$$

By Lemma 3.14, the $d(u)$ dimensional state vectors $\bar{u}_0(d(u)), \ldots, \bar{u}_{d(u,T(u))}(d(u))$ are strongly dependent modulo P^s for all $s \ge T(u)$. By Theorem 2.10, this yields that $\bar{u}_0(d(u))), \ldots, \bar{u}_{d(u,T(u))}(d(u))$ are dependent over R. However, by Lemma 3.16, the vectors $\bar{u}_0(d(u)), \ldots, \bar{u}_{d(u)-1}(d(u))$ are independent, thus

$$d(u) - 1 < d(u, T(u)) \ . \quad \square$$

The following lemma shows that every linear recurring sequence can be split into two parts: a dominating and a less important recurring sequence.

Lemma 3.18. *Let R be a Dedekind-domain, $P \subseteq R$ be a prime ideal with finite norm, let u be a l.r.s. over R and let $t, s \in \mathbb{N}$.*

Then there exist linear recurring sequences $u^{(1)}$ and $u^{(2)}$, such that

$$u \equiv u^{(1)} + u^{(2)} \mod P^s \ ,$$

$$u^{(2)} \equiv 0 \mod P^t \ ,$$

$$T(u^{(1)}) \le t \ ,$$

$$d(u^{(1)}) = d(u, t)$$

and

$$d(u^{(2)}) \le 2d(u) \ .$$

Proof. Let

$$u_n^{(1)} = u_n \quad \text{for} \quad n = 0, \dots, d(u,t) - 1$$

and define $u_n^{(1)}$ for $n \geq d(u,t)$ by the recurrence relation

$$\bar{u}_n^{(1)}(d(u,t)) = M(u,t)^n \bar{u}_0^{(1)}(d(u,t)) \ .$$

Then

$$u_n \equiv u_n^{(1)} \mod P^t \quad \text{holds for all } n \geq 0 \ .$$

Thus

$$\nu_P(u_n - u_n^{(1)}) \geq t$$

and we can define

$$u_n^{(2)} = (u_n - u_n^{(1)}) \ .$$

For this sequences

$$u = u^{(1)} + u^{(2)} \quad \text{and} \quad u^{(2)} \equiv 0 \mod P^t$$

obviously holds. It is also clear that

$$T(u^{(1)}) \leq t$$

and by Lemma 3.17,

$$d(u^{(1)}) = d(u^{(1)}, t) = d(u,t) \ .$$

By Lemma 3.8, the sequence $u^{(2)}$ is a l.r.s. with

$$d(u^{(2)}) \leq d(u^{(1)}) + d(u) \leq 2d(u) \ . \quad \square$$

In the next lemmas we prove some properties of the period length and the lifting of the differences of elements of the recurring sequences to the expanded residue class systems.

Lemma 3.19. *Let R be a Dedekind-domain, $P \subseteq R$ be a prime ideal with finite norm, let u be a l.r.s. over R and suppose that*

$$d(u,s) = d(u, s+k) = d \quad \textit{for some} \quad k \geq 0 \ .$$

Furthermore, let $a_{s+k,d-1}, \dots, a_{s+k,0}$ be as in Definition 1.17. Let $b_0, \dots, b_{d-1} \in R$ and let

$$b_{n+d} = a_{s+k,d-1} b_{n+d-1} + \dots + a_{s+k,0} b_n \quad \textit{for} \quad n \geq 0 \ .$$

Then

$$\varrho(b, k+1) \mid \varrho(u, s+k) \ .$$

Proof. In the proof we will use the notations:

$$\bar{u}_n = \bar{u}_n(d(u,s)) \ , \quad \varrho = \varrho(u, s+k)$$
$$\text{and}$$
$$M = M(u, s+k) \ .$$

By Lemma 3.13, the $d(u,s) = d$ dimensional state vectors $\bar{u}_0, \ldots, \bar{u}_{d-1}$ form a semi-basis modulo P^s and P^{s+k}.

By Theorem 2.16, there exist for every $\bar{b} \in V(R,d)$ coefficients $\lambda_0, \ldots, \lambda_{d-1} \in R$ and $p \in P^{s-1}$, such that

$$p\bar{b} \equiv \lambda_0\bar{u}_0 + \cdots + \lambda_{d-1}\bar{u}_{d-1} \mod P^{s+k} \ . \tag{3.4}$$

By the definition of ϱ we have

$$\bar{u}_{n+\varrho} \equiv \bar{u}_n \mod P^{s+k} \ ,$$

i.e.

$$M^{\varrho}\bar{u}_n \equiv \bar{u}_n \mod P^{s+k} \ .$$

Hence, using (3.4) and the definition of the sequence b, we get

$$\begin{aligned} p\bar{b}_{\varrho+n} &\equiv pM^{\varrho+n}\bar{b}_0 \equiv pM^{\varrho+n}\bar{b} \\ &\equiv M^{\varrho+n}\lambda_0\bar{u}_0 + \cdots + M^{\varrho+n}\lambda_{d-1}\bar{u}_{d-1} \\ &\equiv M^n\lambda_0\bar{u}_0 + \cdots + M^n\lambda_{d-1}\bar{u}_{d-1} \\ &\equiv pM^n\bar{b} \equiv pM^n\bar{b}_0 \equiv p\bar{b}_n \mod P^{s+k} \ . \end{aligned}$$

But this means that ϱ is a period length of the sequence b modulo P^{k+1} and thus $\varrho(b, k+1) \mid \varrho$. □

Lemma 3.20. *Let R be a Dedekind-domain, $P \subseteq R$ be a prime ideal with finite norm, let u be a l.r.s. over R, $s \geq T(u)$ and let $l, n \in \mathbb{N}$. Then*

$$u_{n+l\varrho(u,s)} - u_n \equiv l(u_{n+\varrho(u,s)} - u_n) \mod P^{s+1} \ .$$

Proof. Let

$$\bar{u}_n = \bar{u}_n(d(u)) \ , \quad M = M(u) \ , \quad \varrho = \varrho(u,s)$$
$$\text{and let}$$
$$y_n = u_{n+\varrho} - u_n \ , \quad \bar{y}_n = \bar{y}_n(d(u)) \ .$$

Clearly,

$$\bar{y}_n = M^n\bar{y}_0 \ ,$$

and since

$$u_{n+\varrho} \equiv u_n \mod P^s \ ,$$

the relation $y_n \in P^s$ holds.

Let $p \in P^s \setminus P^{s+1}$. By Corollary 2.6 there exist $b_0, \ldots, b_{d(u)-1} \in R$, such that

$$y_i \equiv pb_i \mod P^{s+1} \quad \text{for} \quad i = 0, \ldots, d(u)-1 \ .$$

Let us define the sequence b_n by $\bar{b}_n = M^n \bar{b}_0$. Then clearly,

$$pb_n \equiv y_n \mod P^{s+1} \ .$$

By Lemma 3.17, we have $d(u,s) = d(u)$. Hence by setting $k = 0$ in Lemma 3.19, we find that $\varrho(b,1) \mid \varrho$, whence

$$M^{i\varrho}\bar{b}_n \equiv \bar{b}_n \mod P$$

and thus

$$M^{i\varrho}\bar{y}_n \equiv \bar{y}_n \mod P^{s+1}$$

for any $i \in \mathbb{N}$.

Let E denote the $d(u)$ dimensional unit matrix. Then we have

$$\begin{aligned}
\bar{u}_{n+l\varrho} - \bar{u}_n &\equiv (M^{l\varrho} - E)\bar{u}_n \\
&\equiv \left(\sum_{i=0}^{l-1} M^{i\varrho}\right)(M^{\varrho} - E)\,\bar{u}_n \\
&\equiv \left(\sum_{i=0}^{l-1} M^{i\varrho}\right)\bar{y}_n \\
&\equiv \sum_{i=0}^{l-1} \left(M^{i\varrho}\bar{y}_n\right) \\
&\equiv l\bar{y}_n \equiv l\left(\bar{u}_{n+\varrho} - \bar{u}_n\right) \mod P^{s+1} \ . \quad \square
\end{aligned}$$

Lemma 3.21. *Let R be a Dedekind-domain, $P \subseteq R$ be a prime ideal, let $\pi \in \mathbb{N}$ be the prime, such that $\pi \mid N(P)$, let u be a l.r.s. over R and let $s \in \mathbb{N}$.*

If $s \geq T(u)$, then either

$$\varrho(u, s+1) = \varrho(u,s)$$

or

$$\varrho(u, s+1) = \pi\,\varrho(u,s) \ .$$

Proof. Let us define the sequence $y^{(l)}$ by

$$y_n^{(l)} = u_{n+l\varrho(u,s)} - u_n$$

and use the notation

$$\bar{y}_n^{(l)} = \bar{y}_n^{(l)}(d(u)) \ \text{ and } \ M = M(u) \ .$$

For this $\bar{y}^{(l)}$ clearly,

$$\bar{y}_n^{(l)} \equiv 0 \mod P^s$$

and

$$\bar{y}_{n+i}^{(l)} = M^i \bar{y}_n^{(l)} \text{ for all } i \in \mathbb{N} .$$

Hence, if

$$\bar{y}_n^{(1)} \equiv 0 \mod P^{s+1} \text{ for some } n \in \mathbb{N} ,$$

then

$$\bar{y}_{n+i}^{(1)} \equiv 0 \mod P^{s+1} \text{ for all } i \in \mathbb{N} ,$$

and

$$\varrho(u, s+1) = \varrho(u, s) .$$

Thus, if we assume that

$$\varrho(u, s+1) > \varrho(u, s) ,$$

then

$$\bar{y}_n^{(1)} \not\equiv 0 \mod P^{s+1} .$$

By Lemma 3.20, we have

$$\bar{y}_n^{(l)} \equiv l\bar{y}_n^{(1)} \mod P^{s+1} ,$$

whence

$$\bar{y}_n^{(l)} \equiv 0 \mod P^{s+1} \text{ if and only if } \pi \mid l .$$

From this, we get that the smallest positive value for l, such that

$$u_{n+l\varrho(u,s)} \equiv u_n \mod P^{s+1}$$

is

$$l = \pi . \quad \square$$

Remark 3.22. *Ward in his Theorem 7.1. of* [20] *claimed that for a third-order l.r.s. the statment of Lemma 3.21 remains true even if we omit the condition* $s \geq T(u)$. *However, this is false, as shown e.g. by the sequence* $u_n = 5F_n$ *with* $P = (5) \subseteq \mathbb{Z} = R$ *and* $s = 1$, *where* F_n *is the Fibonacci sequence. The period length of* $5F_n$ *modulo* 5 *is* 1 *while modulo* 25 *is* 20.

Lemma 3.23. *Let* R *be a Dedekind-domain,* $P \subseteq R$ *be a prime ideal, let* $t \in \mathbb{N}$ *and let* u *be a l.r.s. over* R, *such that*

$$u_n \equiv 0 \mod P^t \quad \textit{for all} \quad n \in \mathbb{N} .$$

Furthermore, let $s \geq 0$, $z \geq 1$ *be integers and*

$$N(P) = \pi^z \quad \textit{with} \quad \pi \in \mathbb{N} \quad \textit{prime.}$$

Then

$$\varrho(u, s+t) < \pi^{zd(u)+s-1} .$$

Proof. Let v be the sequence satisfying the same recurrence relation as u with initial values

$$v_0 = 0, \dots, v_{d(u)-2} = 0, v_{d(u)-1} = 1 \ .$$

Then $\bar{v}_0(d(u)), \dots, \bar{v}_{d(u)-1}(d(u))$ are linearly independent modulo P, whence by Lemma 3.14, we find that

$$d(v) = d(u) \le d(v, 1) \ .$$

Thus $T(v) = 1$ and by Lemma 3.21, we have

$$\varrho(v, s) \mid \varrho(v, 1)\pi^{s-1} \ .$$

Let $p \in P^t \setminus P^{t+1}$. By Theorem 2.3 there exist a sequence $u'_0, u'_1, \dots \in R$, such that

$$u_n \equiv pu'_n \mod P^{s+t} \quad \text{for all} \quad n \in \mathbb{N} \ .$$

This sequence u' is not necessarily a l.r.s, but periodic modulo P^s with

$$\varrho(u', s) = \varrho(u, s + t)$$

and

$$p\bar{u}'_n(d(u)) \equiv M(u)^n p\bar{u}'_0(d(u)) \mod P^{s+t} \ ,$$

whence

$$\bar{u}'_n(d(u)) \equiv M(u)^n \bar{u}'_0(d(u)) \mod P^s \ .$$

Since $\bar{u}'_0(d(u))$ is a linear combination of the vectors $\bar{v}_0(d(u)), \dots, \bar{v}_{d(u)-1}(d(u))$ (with coefficients in R),

$$\varrho(u, s + t) = \varrho(u', s) \mid \varrho(v, s) \ .$$

We know that

$$\varrho(v, 1) < \pi^{zd(u)}$$

whence

$$\varrho(u, s + t) \le \varrho(v, s) \le \varrho(v, 1)\pi^{s-1} < \pi^{zd(u)}\pi^{s-1} \ . \quad \square$$

As an application of the lemmas above, we can prove the following fundamental theorem:

Theorem 3.24. *Let R be a Dedekind-domain, u be a l.r.s., P be a prime ideal with finite norm in R and $\pi \in \mathbb{N}$ be the prime, such that $\pi \mid N(P)$.*

If u is uniformly distributed modulo P^s for all $s \in \mathbb{N}$, then $N(P) = \pi$.

Proof. Suppose that

$$N(P) = \pi^z \quad \text{with} \quad z \in \{1, 2, 3, \dots\} \ .$$

Fix $s = 2d(u)$. For this s there are $(\pi^z)^s = \pi^{zs}$ different residue classes modulo P^s. Since u is u.d. modulo P^s, thus $\pi^{sz} \le \varrho(u, s)$. Hence by Lemma 3.23

$$\pi^{sz} \le \varrho(u, s) < \pi^{zd(u)+s-1} \ ,$$

and substituting the value of s, the inequality has the form

$$\pi^{2zd(u)} < \pi^{zd(u)+2d(u)-1} .$$

Taking the logarithm of both sides we obtain

$$2zd(u) < zd(u) + 2d(u) - 1 < zd(u) + 2d(u) ,$$

whence canceling $d(u)$ out, we find

$$2z < z + 2 , \quad \text{i.e.} \quad z < 2 . \qquad \square$$

Now we can turn to the generalization of the results related to the period length and lifting properties.

Lemma 3.25. *Let $t, k, \pi \in \mathbb{N}$, where π is a prime, R be a Dedekind-domain, $P \subseteq R$ be a prime ideal with finite norm, such that $\pi \mid N(P)$ and let u and v be two linear recurring sequences over R, such that*

$$v_n \equiv 0 \mod P^t \quad \textit{for all} \quad n \in \mathbb{N} .$$

Suppose that there exists $T_0 > T(u)$, such that

$$\nu_\pi(\varrho(v, t+k+i+1)) < \nu_\pi(\varrho(u, T_0+i)) \quad \textit{for all} \quad i \geq 0$$

and set

$$\Lambda' = \varrho(v, T(v))/\gcd(\varrho(u, T_0), \varrho(v, T(v)) \quad \textit{and} \quad \Lambda = \Lambda'/\pi^{\nu_\pi(\Lambda')} .$$

Let $s \geq T_0 + k$, such that

$$\varrho(u, s+1) = \pi\varrho(u, s)$$

and suppose that $t \geq T_0$.

Then the congruence

$$\begin{aligned} (u+v)_{n+m\varrho(u,s)+ql\Lambda\varrho(u,s+1)} - (u+v)_{n+m\varrho(u,s)} \\ \equiv \pi l\Lambda(u_{n+q\varrho(u,s)} - u_n) \mod P^{s+k+1} \end{aligned} \tag{3.5}$$

holds for all $n, m, l, q \geq 0$.

Proof. The case $l = 0$ is trivial.

Suppose that $l > 0$ and let

$$M = M(u) * M(v) \in V(R, d \times d) ,$$

where $*$ denotes the operation defined in Remark 3.11 and d is the dimension of M. Furthermore, let

$$y_n = (u_{n+q\varrho_1} - u_n) ,$$

let E be the d dimensional unit matrix and write

$$\bar{u}_n = \bar{u}_n(d) \ , \quad \bar{v}_n = \bar{v}_n(d) \ , \quad \bar{y}_n = \bar{y}_n(d) \ ,$$
$$\varrho_1 = \varrho(u,s) \ , \quad \varrho_2 = \varrho(u,s+1) \ .$$

By the definition of ϱ_1, we have

$$y_n \equiv 0 \mod P^s \ .$$

Hence by Corollary 2.6 there exist $b_0, \dots, b_{d-1} \in R$, such that

$$y_i \equiv pb_i \mod P^{s+k+1} \quad \text{for} \quad i = 0, \dots, d-1 \ .$$

Let us define the sequence b_n by $\bar{b}_n = M^n \bar{b}_0(d)$. Then clearly,

$$pb_n \equiv y_n \mod P^{s+k+1} \ .$$

Since $d(s) = d(s-k)$ by Lemma 3.19

$$\varrho(b, k+1) \mid \varrho_1 \ ,$$

i.e.

$$M^{\varrho_1} \bar{b}_n \equiv \bar{b}_n \mod P^{k+1}$$

and thus

$$M^{\varrho_1} \bar{y}_n \equiv \bar{y}_n \mod P^{s+k+1} \ , \tag{3.6}$$

whence

$$\left(\sum_{i=0}^{\pi l \Lambda - 1} M^{iq\varrho_1} \right) \bar{y}_n \equiv \pi l \Lambda \bar{y}_n \mod P^{s+k+1} \ . \tag{3.7}$$

Using similar arguments as in the proof of Lemma 3.20, by (3.6) and (3.7) we have

$$\begin{aligned}
&(\bar{u}+\bar{v})_{n+m\varrho_1+lq\Lambda\varrho_2} - (\bar{u}+\bar{v})_{n+m\varrho_1} \\
&\equiv M^{m\varrho_1}(M^{lq\Lambda\varrho_2} - E)(\bar{u}+\bar{v})_n \\
&\equiv M^{m\varrho_1}(M^{lq\Lambda\pi\varrho_1} - E)\bar{u}_n + M^{m\varrho_1}(M^{lq\Lambda\varrho_2} - E)\bar{v}_n \\
&\equiv M^{m\varrho_1} \left(\sum_{i=0}^{l\Lambda\pi-1} M^{iq\varrho_1} \right) (M^{q\varrho_1} - E)\, \bar{u}_n + M^{m\varrho_1}(M^{lq\Lambda\varrho_2} - E)\bar{v}_n \\
&\equiv \left(\sum_{i=0}^{l\Lambda\pi-1} M^{iq\varrho_1} \right) M^{m\varrho_1} \bar{y}_n + M^{m\varrho_1}(M^{lq\Lambda\varrho_2} - E)\bar{v}_n \\
&\equiv \left(\sum_{i=0}^{l\Lambda\pi-1} M^{iq\varrho_1} \right) \bar{y}_n + M^{m\varrho_1}(M^{lq\Lambda\varrho_2} - E)\bar{v}_n \\
&\equiv l\Lambda\pi \bar{y}_n + M^{m\varrho_1}(M^{lq\Lambda\varrho_2} - E)\bar{v}_n \\
&\equiv l\Lambda\pi \, (u_{n+q\varrho_1} - u_n) + M^{m\varrho_1}(M^{lq\Lambda\varrho_2} - E)\bar{v}_n \mod P^{s+k+1} \ .
\end{aligned} \tag{3.8}$$

Now, we show that $M^{m\varrho_1}(M^{lq\Lambda\varrho_2} - E)\bar{v}_n$ vanishes in the congruence (3.8). Let us observe the following three cases:

i.) If $t > s + k$, then

$$\bar{v}_n \equiv 0 \mod P^{s+k+1} .$$

ii.) If $s < t \leq s + k$, then

$$\varrho(v, s+k+1) \mid \varrho(v, t+k+1) \mid \Lambda\varrho(u, T_0) \mid \Lambda\varrho(u, s) \mid \Lambda\varrho_2 ,$$

whence

$$(M^{lq\Lambda\varrho_2} - E)\bar{v}_n \equiv 0 \mod P^{s+k+1} . \tag{3.9}$$

iii.) Finally, if $t \leq s$, then

$$\varrho(v, s+k+1) = \varrho(v, (s-t)+t+k+1) \mid \Lambda\varrho(u, T_0+s-t) \mid \Lambda\varrho(u, s) \mid \Lambda\varrho_2 ,$$

whence again (3.9) follows.

Applying the above observation to (3.8) we obtain (3.5). □

Corollary 3.26. *With the assumptions of Lemma 3.25, we have*

$$\begin{aligned}(u+v)_{n+lq\Lambda\varrho(u,s+1)} - (u+v)_n &\equiv l\left((u+v)_{n+q\Lambda\varrho(u,s+1)} - (u+v)_n\right) \\ &\equiv l\Lambda(u_{n+q\varrho(u,s+1)} - u_n) \qquad \mod P^{s+k+1} .\end{aligned}$$

Proof. By Lemma 3.25, we can write

$$\begin{aligned}&(u+v)_{n+m\varrho(u,s)+ql\Lambda\varrho(u,s+1)} - (u+v)_{n+m\varrho(u,s)} \\ &\qquad \equiv l\left(\pi\Lambda(u_{n+q\varrho(u,s)} - u_n)\right) \\ &\qquad \equiv l\left((u+v)_{n+q\Lambda\varrho(u,s+1)} - (u+v)_n\right) \mod P^{s+k+1} .\end{aligned}$$

Set the sequence $v'_n = 0$. Then

$$\begin{aligned}&(u+v)_{n+m\varrho(u,s)+ql\Lambda\varrho(u,s+1)} - (u+v)_{n+m\varrho(u,s)} \\ &\qquad \equiv l\Lambda\left(\pi(u_{n+q\varrho(u,s)} - u_n)\right) \\ &\qquad \equiv l\Lambda\left((u+v')_{n+q\varrho(u,s+1)} - (u+v')_n\right) \\ &\qquad \equiv l\Lambda(u_{n+q\varrho(u,s+1)} - u_n) \qquad \mod P^{s+k+1} . \quad \square\end{aligned}$$

As a consequence of the above results we can prove that a linear recurring sequence is either periodic or if s is greater than a given bound, the period length of the sequence modulo P^s is strictly increasing with s.

Theorem 3.27. *Let $\pi \in \mathbb{N}$ be a prime, R be a Dedekind-domain, $P \subseteq R$ be a prime ideal with finite norm, such that $\pi \mid N(P)$, let u be a l.r.s. over R and $s > T(u)$ be an integer.*

If

$$\varrho(u, s+1) = \pi\,\varrho(u, s) \ ,$$

then

$$\varrho(u, s+2) = \pi\,\varrho(u, s+1) \ .$$

Proof. Let $\bar{u}_n = \bar{u}_n(d(u))$. Setting $k = 1$, $v_n = 0$, $m = 0$, $l = 1$ and $q = 1$ in Lemma 3.25, we obtain that

$$\bar{u}_{n+\varrho(u,s+1)} - \bar{u}_n \equiv \pi(\bar{u}_{n+\varrho(u,s)} - \bar{u}_n) \mod P^{s+2} \ .$$

Since $\varrho_{s+1} > \varrho_s$, we have

$$\bar{u}_{n+\varrho(u,s)} - \bar{u}_n \not\equiv 0 \mod P^{s+1}$$

and thus

$$\bar{u}_{n+\varrho(u,s+1)} - \bar{u}_n \not\equiv 0 \mod P^{s+2} \ .$$

Hence by Lemma 3.21, we get

$$\varrho(u, s+2) = \pi\,\varrho(u, s+1) \ . \quad \square$$

In the following corollary we prove that the required existence of T_0 in Lemma 3.25 is not a real restriction.

Corollary 3.28. *Let R be a Dedekin-domain, $\pi \in \mathbb{N}$ be a prime, $P \subseteq R$ be a prime ideal, such that $\pi \mid N(P)$, let u and v be linear recurring sequences over R, such that u is non-periodic and $v_n \equiv 0 \mod P^t$ with some $t \in \mathbb{N}$ for all $n \in \mathbb{N}$ and let $k \in \mathbb{N}$.*

Then there exists $T_0 \in \mathbb{N}$, such that

$$\nu_\pi(\varrho(v, t+k+i+1)) < \nu_\pi(\varrho(u, T_0+i)) \quad \textit{for all} \quad i \geq 0 \ .$$

Proof. Satisfying

$$\nu_\pi(\varrho(v, t+k+i+1)) < \nu_\pi(\varrho(u, T_0+i)) \quad \text{for all} \quad i \geq 0 \ ,$$

it is enough to choose T_0, such that

$$\varrho(u, T_0+1) = \pi\,\varrho(u, T_0)$$

and

$$\nu_\pi(\varrho(v, t+k+i+1)) < \nu_\pi(\varrho(u, T_0+i)) \quad \text{for} \quad 0 \leq i \leq T(v) - t \ .$$

If $i > T(v) - t$, then the property follows from Lemma 3.21 and Corollary 3.27. $\square$

In the following remark we give some estimation for T_0 in the most important cases.

Remark 3.29. *Assume that* $N(P) = \pi$.

a.) By Lemma 3.23, we have

$$\nu_\pi(\varrho(v, t+k+i+1)) \le d(v) + k + i - 1$$

and if we suppose that u *is uniformly distributed modulo* P^{T_0+i}, *then*

$$T_0 + i \le \nu_\pi(\varrho(u, T_0 + i)) \ .$$

If $T_0 \ge d(v) + k$, *then*

$$\begin{aligned} \nu_\pi(\varrho(v, t+k+i+1)) &\le d(v) + 1 + k + i - 2 \\ &< T_0 + i \\ &\le \nu_\pi(\varrho(u, T_0 + i)) \ . \end{aligned}$$

b.) Further, again by Lemma 3.23, we have

$$\nu_\pi(\varrho(u, T(u))) \le d(u) + T(u) - 2 \ .$$

Thus

$$T_0 \le \nu_\pi(\varrho(u, T_0)) \ ,$$

provided that u *is uniformly distributed modulo* P^{T_0}.

If

$$T_0 \ge d(u) + T(u) - 1 \ ,$$

then

$$\nu_\pi(\varrho(u, T(u))) \le d(u) + T(u) - 2 < T_0 \le \nu_\pi(\varrho(u, T_0)) \ .$$

This yields that there exists an $i \in \mathbb{N}$ *with* $T(u) \le i < T_0$, *such that*

$$\nu_\pi(\varrho(u, i)) < \nu_\pi(\varrho(u, i+1)) \ ,$$

whence by Lemma 3.21, we get

$$\nu_\pi(\varrho(u, i)) + 1 \le \nu_\pi(\varrho(u, i+1)) \ .$$

Using Theorem 3.27, we obtain by induction that

$$\nu_\pi(\varrho(u, T_0)) + j \le \nu_\pi(\varrho(u, T_0 + j)) \quad \textit{for all} \quad j \ge 0 \ .$$

c.) Let $T' = \max\{d(v) + k, d(u) + T(u) - 1\}$. *If* u *is u.d. modulo* $P^{T'+1}$, *then we can choose* $T_0 = T'$ *in Lemma 3.24.*

Remark 3.30. *Using the notations of Lemma 3.25, we find that* $\varrho(u + v, s + 1)$ *divides* $\pi\Lambda\varrho(u, s)$, *which comes from Theorem 3.27 and the congruence* (3.5) *modulo* P^{s+1}.

In the lemma below we give a lower bound on the distance of the elements corresponding to the same residue class of a uniformly distributed linear recurring sequence.

Lemma 3.31. *Let R be a Dedekin-domain, $\pi \in \mathbb{N}$ be a prime, $P \subseteq R$ be a prime ideal, such that $\pi \mid N(P)$, u be a l.r.s. over R, let $l, s \in \mathbb{N}$, such that*

$$s > T(u) + d(u) \quad \textit{and} \quad \pi \nmid l$$

and suppose that

$$\varrho(u, s) = \pi\, \varrho(u, s-1) \ .$$

If

$$u_n \equiv u_{n+l\varrho(u,s)} \mod P^{s+d(u)} \quad \textit{for some} \quad 0 \le n \ ,$$

then u cannot be u.d. modulo $P^{s+d(u)}$.

Proof. Setting $v_n = 0$, $T_0 = T(u)$ and $k = d(u)$, by Lemma 3.26,

$$u_{n+l\varrho(u,s)} - u_n \equiv l(u_{n+\varrho(u,s)} - u_n) \mod P^{s+d(u)} \ .$$

Since $\pi \nmid l$, there exists $l^{-1} \in R$, such that

$$ll^{-1} \equiv 1 \mod P^{s+d(u)} \ .$$

This yields

$$u_{n+m\varrho(u,s)} - u_n \equiv ml^{-1}(u_{n+l\varrho(u,s)} - u_n) \equiv 0 \mod P^{s+d(u)} \ ,$$

for every $m \ge 0$.

By Theorem 3.27 we know that

$$\varrho(u, s + d(u)) = \pi^{d(u)} \varrho(u, s) \ .$$

This means that $u_n, \ldots, u_{n+\varrho(u,s+d(u))-1}$ contains at least $\pi^{d(u)}$ elements in the residue class of u_n modulo $P^{s+d(u)}$.

Suppose that the sequence is uniformly distributed modulo $P^{s+d(u)}$. Then among $u_n, \ldots, u_{n+\varrho(u,s+d(u))-1}$, every residue class modulo $P^{s+d(u)}$ appear with the same frequency. The number of different residue classes modulo $P^{s+d(u)}$ is

$$N(P)^{s+d(u)} = \pi^{z(s+d(u))} \quad \text{with some} \quad z \ge 1 \ ,$$

thus

$$\varrho(u, s + d(u)) \ge \pi^{z(s+d(u))}\pi^{d(u)} \ge \pi^{s+d(u)}\pi^{d(u)} = \pi^{s+2d(u)} \ .$$

On the other hand, by Lemma 14,

$$\varrho(u, s + d(u)) < \pi^{s+2d(u)-1} \ ,$$

which is a contradiction. □

The following fundamental theorem gives the very important lifting property of the uniform distribution.

Theorem 3.32. *Let R be a Dedekind-domain, $\pi \in \mathbb{N}$ be a prime, let u and v be two linear recurring sequences over R, $P \subseteq R$ a prime ideal with $N(P) = \pi$, let T_0, t and Λ as in Lemma 3.25 and let*

$$s \geq T_0 + 2d(u) \ .$$

If u and $u+v$ are uniformly distributed modulo P^s, then the sequence $u+v$ is also uniformly distributed modulo P^{s+1}.

Proof. We will construct a partition $\mathfrak{H}$ of the set $\{0, \ldots, \Lambda\varrho(u, s+1)-1\}$, such that if $A \in \mathfrak{H}$, then

$$u_n \equiv u_m \mod P^s \quad \text{for all} \quad n, m \in A$$

and if

$$a \equiv b \mod P^s$$

then

$$\#\{n \in A \mid (u+v)_n \equiv a \mod P^{s+1}\} = \#\{n \in A \mid (u+v)_n \equiv b \mod P^{s+1}\} \ .$$

If we can find such a partition, then u and $u+v$ are also uniformly distributed modulo P^{s+1}.

Construct first the following class of sets:

$$A_{n,l} = \{i \mid i \equiv n \mod \Lambda\varrho(u, s-l) \text{ and } 0 \leq i < \Lambda\varrho(u, s+1)\} \ ,$$

where

$$0 \leq l < d(u) \quad \text{and} \quad 0 \leq n < \Lambda\varrho(u, s-l) \ .$$

Since we know that the period lengths

$$\varrho(u, s+1) = \pi^{l+1}\varrho(u, s-l) \ ,$$

the cardinality of the sets

$$\#A_{n,l} = \pi^{l+1}$$

and

$$A_{n,l} = A_{m,r} \quad \text{if and only if} \quad n = m \quad \text{and} \quad l = r \ .$$

Define the partition $\mathfrak{H}$ with the help of the above sets:

$$\mathfrak{H} = \{A_{n,l} \mid \forall i, j \in A_{n,l} \ , \ u_i \equiv u_j \mod P^s \text{ and} \\ \exists i, j \in A_{n,l}, \text{ such that } u_i \not\equiv u_j \mod P^{s+1}\} \ .$$

The proof proceeds in two steps.

In step a.) we will prove that $\mathfrak{H}$ is a partition of $\{0, \ldots, \Lambda\varrho(u, s+1)-1\}$ and in step b.) we will prove that if

$$A_{n,l} \in \mathfrak{H} \quad \text{and} \quad a \equiv b \mod P^s \ ,$$

then

$$\#\{m \in A_{n,l} \,|(u+v)_m \equiv a \mod P^{s+1}\} \\ = \#\{m \in A_{n,l} \mid (u+v)_m \equiv b \mod P^{s+1}\} \ .$$

a.) We claim $\mathfrak{H}$ is a partition of $\{0, \ldots, \Lambda\varrho(u, s+1)-1\}$. Thereto we will prove the followings:

i.) If

$$A_{n,l} \neq A_{m,r} \quad \text{and} \quad A_{n,l} \cap A_{m,r} \neq \emptyset \ ,$$

then

$$l < r \quad \text{and} \quad A_{n,l} \subseteq A_{m,r} \quad \text{or} \quad r < l \quad \text{and} \quad A_{m,r} \subseteq A_{n,l} \ .$$

Assume first that $l = r$. Then

$$A_{n,l} \cap A_{m,r} \neq \emptyset$$

means that there exists an integer i, such that

$$i \equiv n \mod \Lambda\varrho(u, s-l) \quad \text{and} \quad i \equiv m \mod \Lambda\varrho(u, s-l)$$

and consequently

$$m \equiv n \mod \Lambda\varrho(u, s-l) \ .$$

But we know that

$$0 \leq n, m < \Lambda\varrho(u, s-l) \ ,$$

whence

$$n = m \quad \text{and} \quad A_{n,l} = A_{m,r} \ .$$

If $l \neq r$, then we may assume that $l < r$ without loss of generality. In this case

$$A_{n,l} \cap A_{m,r} \neq \emptyset$$

means that there exists an integer i, such that

$$i \equiv n \mod \Lambda\varrho(u, s-l) \quad \text{and} \quad i \equiv m \mod \Lambda\varrho(u, s-r)$$

and since $\varrho(u, s-r) | \varrho(u, s-l)$, thus

$$m \equiv n \mod \Lambda\varrho(u, s-r) \ .$$

Let $j \in A_{n,l}$. Then

$$j \equiv n \mod \Lambda\varrho(u, s-l)$$

and consequently

$$j \equiv n \equiv m \mod \Lambda\varrho(u, s-r) \ ,$$

thus

$$A_{n,l} \subseteq A_{m,r} \ .$$

ii.) If $A_{m,r} \in \mathfrak{H}$, then no subsets of $A_{m,r}$ are contained in $\mathfrak{H}$.

Suppose that

$$A_{m,r} \in \mathfrak{H} \quad \text{and} \quad A_{n,l} \subsetneq A_{m,r} \ .$$

By (i) we have $l < r$. Let m' be such that

$$m' \equiv n \mod \Lambda\varrho(u, s-r+1) \quad \text{and} \quad 0 \leq m' < \Lambda\varrho(u, s-r+1) \ .$$

We will show that

$$A_{n,l} \subseteq A_{m',r-1} \subsetneq A_{m,r} \ .$$

By the definition of m' and $A_{m',r-1}$, we know that $n \in A_{m',r-1}$, which means that

$$A_{m',r-1} \cap A_{n,l} \neq \emptyset$$

and by (i) we have

$$A_{n,l} \subseteq A_{m',r-1} \ .$$

This yields that

$$A_{m',r-1} \cap A_{m,r} \neq \emptyset$$

and again by (i) we find

$$A_{m',r-1} \subseteq A_{m,r} \ .$$

Since

$$\#A_{m',r-1} \neq \#A_{m,r} \ ,$$

thus

$$A_{m',r-1} \subsetneq A_{m,r} \ .$$

We claim that if $i \in A_{n,l}$, then $u_i \equiv u_{m'} \mod P^{s+1}$.
Let $i \in A_{n,l}$. Since

$$A_{n,l} \subseteq A_{m',r-1} \ ,$$

thus $i \in A_{m',r-1}$ and there exists an integer a, such that

$$i = m' + a\Lambda\varrho(u, s-r+1) \ .$$

If we set

$$v_n = 0 \ , \quad k = d(u) \ , \quad l = a \quad \text{and} \quad q = \Lambda \ ,$$

by Lemma 3.25 we obtain

$$u_i - u_{m'} \equiv \pi a \left(u_{m'+\Lambda\varrho(u,s-r)} - u_{m'}\right) \mod P^{s-r+d(u)+1} \ ,$$

whence

$$u_i - u_{m'} \equiv \pi a \left(u_{m'+\Lambda\varrho(u,s-r)} - u'_m\right) \mod P^{s+1} \ .$$

Since

$$A_{m',r-1} \subseteq A_{m,r}$$

and

$$0 \leq m' + \Lambda\varrho(u, s-r) \leq i < \Lambda\varrho(u, s+1) \ ,$$

thus

$$m', m' + \Lambda\varrho(u, s-r) \in A_{m,r} \ .$$

But $A_{m,r} \in \mathfrak{H}$, whence

$$u_{m'} \equiv u_{m'+\Lambda\varrho(u,s-r)} \mod P^s \ .$$

This yields

$$\pi(u_{m'+\Lambda\varrho(u,s-r)} - u_{m'}) \equiv 0 \mod P^{s+1} \ ,$$

i.e.

$$u_i \equiv u_{m'} \mod P^{s+1} \ .$$

Hence,

$$u_i \equiv u_{m'} \equiv u_j \mod P^{s+1} \quad \text{for every} \quad i, j \in A_{n,l} \ ,$$

and thus $A_{n,l} \notin \mathfrak{H}$.

iii.) Finally we prove that

$$\bigcup_{A \in \mathfrak{H}} A = \{0, \ldots, \Lambda\varrho(u, s+1) - 1\} \ .$$

During step iii.) we will use the notation

$$d = d(u) \quad \text{and} \quad \varrho(i) = \varrho(u, s-d+1+i) \ .$$

We will construct a sequence of partitions $\mathfrak{H}_0, \mathfrak{H}_1, \ldots$, such that

$$\bigcup_{A \in \mathfrak{H}_i} A = \{0, \ldots, \Lambda\varrho(u, s+1) - 1\} \ ,$$

$\mathfrak{H}_{i+1}$ is a refinement of $\mathfrak{H}_i$ and $\mathfrak{H} = \mathfrak{H}_{d-1}$. (Actually, it is not necessary that every $\mathfrak{H}_i$ is a partition of $\{0, \ldots, \Lambda\varrho(u, s+1) - 1\}$, but obviously they are.)

Let

$$\mathfrak{H}_0 = \{A_{n,d-1} | 0 \le n < \Lambda\varrho(0)\} \ .$$

Assuming that we have already defined $\mathfrak{H}_i$, we define $\mathfrak{H}_{i+1}$ by the following:

Let

$$\mathfrak{H}_i' = \{A | A \in \mathfrak{H}_i \text{ and } \exists j_1, j_2 \in A : u_{j_1} \not\equiv u_{j_2} \mod P^s\}$$

and let

$$\mathfrak{H}_{i+1} = (\mathfrak{H}_i \setminus \mathfrak{H}_i') \cup \left(\bigcup_{A_{n,r} \in \mathfrak{H}_i'} \{A_{n+a\Lambda\varrho(u,s-r),r-1} | 0 \le a < \pi\} \right) \ .$$

A simple observation shows that the elements of $\mathfrak{H}_i'$ have the form $A_{n,d-1-i}$.

First we prove that

$$\bigcup_{A \in \mathfrak{H}_i} A = \{0, \ldots, \Lambda\varrho(u, s+1) - 1\} \quad \text{for all} \quad i \ge 0 \ .$$

Obviously, if $i = 0$, the property holds.

Suppose that

$$\bigcup_{A \in \mathfrak{H}_i} A = \{0, \dots, \Lambda\varrho(u, s+1) - 1\}$$

for a fixed i. Since

$$s - d + 1 + i \geq T_0 + d \geq T(u) + d \quad \text{for every} \quad 0 \leq i \leq d - 1 \ ,$$

by similar considerations as in Remark 3.29.b, we have

$$\varrho(i+1) = \pi\,\varrho(i) \ , \tag{3.10}$$

whence

$$\bigcup_{a=0}^{\pi-1} A_{n+a\Lambda\varrho(i),d-2-i} = A_{n,d-1-i} \ .$$

(All the sets $A_{n+a\Lambda\varrho(i),d-2-i}$ are different, all of them is a subset of $A_{n,d-1-i}$ and comparing the cardinalities, we get the equality.) Hence

$$\bigcup_{A \in \mathfrak{H}_{i+1}} A = \{0, \dots, \Lambda\varrho(u, s+1) - 1\} \ .$$

Now we prove that if $i \geq 0$ and $A \in \mathfrak{H}_i$, then there exist $j_1, j_2 \in A$, such that

$$u_{j_1} \not\equiv u_{j_2} \mod P^{s+1} \ .$$

First let $i = 0$. Since u is u.d. modulo P^s and (3.10) holds, by Lemma 3.31,

$$u_n \not\equiv u_{n+\Lambda\varrho(0)} \mod P^{(s-d+1)+d} \quad \text{for every} \quad 0 \leq n < \Lambda\varrho(0) \ .$$

This means that for every $A_{n,d-1} \in \mathfrak{H}_0$ there exist $j_1, j_2 \in A_{n,d-1}$, such that

$$u_{j_1} \not\equiv u_{j_2} \mod P^{s+1}$$

(e.g. $j_1 = n$ and $j_2 = n + \Lambda\varrho(0)$).

Suppose now that $\mathfrak{H}_i$ has the required property. If $A \in \mathfrak{H}_i \cap \mathfrak{H}_{i+1}$, then obviously there exist $j_1, j_2 \in A$, such that

$$u_{j_1} \not\equiv u_{j_2} \mod P^{s+1} \ .$$

Therefore, let us assume that $A \in \mathfrak{H}_{i+1} \setminus \mathfrak{H}_i$. This yields that

$$A = A_{n,d-2-i} \quad \text{for some} \quad 0 \leq n < \Lambda\varrho(i+1) \ .$$

Let m be such that

$$n \equiv m \mod \Lambda\varrho(i) \quad \text{and} \quad 0 \leq m < \Lambda\varrho(i) \ .$$

For this m we have $A_{m,d-1-i} \in \mathfrak{H}_i \setminus \mathfrak{H}_{i+1}$.

By the definition of $\mathfrak{H}_{i+1}$ there exist $j_1, j_2 \in A_{m,d-1-i}$, such that

$$u_{j_1} \not\equiv u_{j_2} \mod P^s \ .$$

Let us fix $j_1, j_2 \in A_{m,d-1-i}$, such that

$$u_{j_1} \not\equiv u_{j_2} \mod P^s \ ,$$

a_1, a_2, such that

$$j_1 = m + a_1 \Lambda\varrho(i) \quad \text{and} \quad j_2 = m + a_2 \Lambda\varrho(i)$$

and set

$$v = 0 \quad \text{and} \quad k = d \ .$$

Then by Corollary 3.26,

$$\begin{aligned} u_{j_1} - u_{j_2} &= (u_{j_1} - u_m) - (u_{j_2} - u_m) \\ &\equiv a_1(u_{m+\Lambda\varrho(i)} - u_m) - a_2(u_{m+\Lambda\varrho(i)} - u_m) \\ &= (a_1 - a_2)(u_{m+\Lambda\varrho(i)} - u_m) \qquad \mod P^{(s-d+i)+d+1} \ , \end{aligned}$$

whence

$$u_{m+\Lambda\varrho(i)} \not\equiv u_m \mod P^s \tag{3.11}$$

follows.

Setting $v = 0$ and $k = d$, by Lemma 3.25,

$$u_{n+\Lambda\varrho(i+1)} - u_n \equiv \pi(u_{m+\Lambda\varrho(i)} - u_m) \mod P^{(s-d+1+i)+d+1}$$

and by (3.11) we obtain that

$$u_{n+\Lambda\varrho(i+1)} \not\equiv u_n \mod P^{s+1} \ ,$$

whence there exist $j_1, j_2 \in A_{n,d-2-i}$, such that

$$u_{j_1} \not\equiv u_{j_2} \mod P^{s+1}$$

(e.g. $j_1 = n$ and $j_2 = n + \Lambda\varrho(i+1)$).

Finally, we only have to prove that $\mathfrak{H}_{d-1} = \mathfrak{H}$.
Let $i = d - 1$. Then for every $A \in \mathfrak{H}_{d-1}$ there exist $j_1, j_2 \in A$, such that

$$u_{j_1} \not\equiv u_{j_2} \mod P^{s+1} \ .$$

Further, by the definition of $\varrho(u, s)$, we know that

$$u_{n+\varrho(u,s)} - u_n \equiv 0 \mod P^s \ ,$$

i.e.

$$u_{j_1} \equiv u_{j_2} \mod P^s \quad \text{for all} \quad j_1, j_2 \in A_{n,0} \ .$$

If $A_{n,d-1-i} \in \mathfrak{H}_{d-1}$, where $0 \leq i < d-1$, then $A_{n,d-1-i} \in \mathfrak{H}_{d-2}$, too, and by the definition of $\mathfrak{H}_{d-1}$, we have

$$u_{j_1} \equiv u_{j_2} \mod P^s \quad \text{for all} \quad j_1, j_2 \in A_{n,d-1-i} \ .$$

Hence $\mathfrak{H}_{d-1} = \mathfrak{H}$ and thus

$$\bigcup_{A \in \mathfrak{H}} A = \{0, \ldots, \Lambda\varrho(u, s+1) - 1\} \ .$$

b.) Now we turn to the assertion that if $A \in \mathfrak{H}$ and $a \equiv b \mod P^s$, then

$$\begin{aligned} &\#\{n \in A \,|(u+v)_n \equiv a \mod P^{s+1}\} \\ &\qquad = \#\{n \in A \mid (u+v)_n \equiv b \mod P^{s+1}\} \ . \end{aligned}$$

Let $A = A_{m,r}$, $n \in A_{m,r}$ and a be such that $n = m + a\Lambda\varrho(u, s-r)$. Setting $k = d(u)$, by Corollary 3.26,

$$(u+v)_n - (u+v)_m \equiv a(u_{m+\Lambda\varrho(u,s-r)} - u_m) \mod P^{(s-r-1)+d(u)+1} \ .$$

Since $A_{m,r} \in \mathfrak{H}$,

$$u_{m+\Lambda\varrho(u,s-r)} - u_m \equiv 0 \mod P^s \ ,$$

but

$$u_{m+\Lambda\varrho(u,s-r)} - u_m \not\equiv 0 \mod P^{s+1} \ .$$

Let

$$y_m = (u_{m+\Lambda\varrho(u,s-r)} - u_m) \ .$$

Since $r < d(u)$,

$$(u+v)_n - (u+v)_m \equiv a\Lambda y_m \mod P^{s+1} \ ,$$

i.e.

$$(u+v)_n \equiv a\Lambda y_m + (u+v)_m \mod P^{s+1} \ .$$

Since

$$y_m \not\equiv 0 \mod P^{s+1} \ ,$$

$$(u+v)_{n_1} \equiv (u+v)_{n_2} \mod P^{s+1}$$

if and only if the corresponding a_1, a_2 are such that $a_1 \equiv a_2 \mod \pi$.

We know that $A_{m,r}$ has π^{r+1} elements, which yields that a takes values from $[0, p^{r+1}-1]$. Since every residue classes modulo π appears pi^r times in $[0, \pi^{r+1}-1]$, thus all the residue classes modulo P^{s+1} which appear in $\{(u+v)_n | n \in A_{m,r}\}$ have π^r representatives, and this means that the assertion is proved. □

Applying the above theorem, we can prove a similar result, which will be useful when we split the linear recurring sequences into dominant and less dominant parts:

Corollary 3.33. *Let R be a Dedekind-domain, $\pi \in \mathbb{N}$ be a prime, u and v be two linear recurring sequences over R, $P \subseteq R$ be a prime ideal with $N(P) = \pi$, T_0 and Λ as in Lemma 3.25 and $s, t \in \mathbb{N}$, such that*

$$s \geq T_0 + 2d(u) \quad \textit{and} \quad t \geq T(u) + 2d(u) \ .$$

If

$$v \equiv 0 \mod P^t \quad \textit{and} \quad u + v \quad \textit{is u.d.} \mod P^s \ ,$$

then

$$u + v \quad \textit{is u.d.} \mod P^{s+1} \ .$$

Proof. Let $v' = 0$. Then the corresponding T_0' can be chosen to be equal to $T(u)$.

If $s < t$, then $u + v \equiv u \mod P^{s+1}$. Since $T_0 \geq T(u)$ and $u + v'$ are u.d. modulo P^s, by Theorem 3.32, $u + v'$ is also u.d. modulo P^{s+1}. But

$$u + v' \equiv u \equiv u + v \mod P^{s+1} \ .$$

If $s \geq t$, then since $u + v \equiv u \mod P^t$, u is u.d. modulo P^t.
Since $t \geq T(u) + 2d(u)$, applying Theorem 3.32 and supposing that u and $u + v'$ are u.d. modulo P^t, then $u + v' = u$ is u.d. modulo P^{t+1}.

Hence by induction u is u.d. modulo P^s, whence again by Theorem 3.32, the statement follows. □

The following lemma proves the existence of splitting the sequences into dominant and less dominant parts:

Lemma 3.34. *Let R be a Dedekind-domain, $\pi \in \mathbb{N}$ be a prime, let u be a linear recurring sequence in R, such that $d(u) \geq 2$ and let $P \subseteq R$ be a prime ideal with $N(P) = \pi$.*

Then there exist an integer $t \geq 0$ and two linear recurring sequences $u^{(1)}$ and $u^{(2)}$ over R, such that

$$u = u^{(1)} + u^{(2)} \ , \quad u^{(2)} \equiv 0 \mod P^t \ , \quad d(u^{(1)}) \leq d(u)$$

$$T(u^{(1)}) \leq \frac{3d(u^{(1)})^2 + d(u^{(1)})}{2} + 2 + d(u)$$

and

$$\max\left\{T(u^{(1)}) + 3d(u^{(1)}) - 1, 4d(u^{(1)}) + d(u)\right\} < t \ .$$

Proof. Let $T_1, \ldots, T_m$ be a set of strictly increasing integers, such that

$$T_1 = 1 \ , \quad T_m = T(u)$$

and

$$d(u, T_{j+1}) > d(u, T_{j+1} - 1) = d(u, T_j) \quad \text{for all} \quad 1 \leq j < m$$

and fix $i \in \mathbb{N}$.

By Lemma 3.18, there exist $v^{(1,i)}$ and $v^{(2,i)}$, such that

$$u = v^{(1,i)} + v^{(2,i)}$$

with

$$v^{(2,i)} \equiv 0 \mod P^{T_{i+1}-1} , \quad T(v^{(1,i)}) \leq T_{i+1} - 1$$

and

$$d(v^{(1,i)}) = d(u, T_{i+1} - 1) = d(u, T_i) .$$

Since

$$v_n^{(1,i)} \equiv u_n \mod P^t \quad \text{for all} \quad n \geq 0$$

and

$$0 \leq t \leq T_{i+1} - 1 ,$$

thus

$$d(v^{(1,i)}, t) = d(u, t) \quad \text{for all} \quad 0 \leq t \leq T_{i+1} - 1 ,$$

whence

$$T(v^{(1,i)}) = T_i .$$

Now suppose that there exist an $1 \leq i' < m$, such that

$$\max \left\{ T_{i'} + 3d(v^{(1,i')}) - 1, 4d(v^{(1,i')}) + d(u) \right\} < T_{i'+1}$$

and fix $i \in \mathbb{N}$ to be the smallest such an i'. Let us also assume that there exists an $1 < l' \leq i$ integer, such that

$$T_{l'-1} + 3d(v^{(1,l'-1)}) - 1 < T_{l'} ,$$

and let l be the maximal among them.

Then by the definition of l,

$$T_j + 3d(v^{(1,j)}) - 1 \geq T_{j+1} \quad \text{for all} \quad l \leq j < i ,$$

whence

$$T_i \leq T_l + \sum_{j=l}^{i-1} (3d(v^{(1,j)}) - 1) .$$

Since

$$d(v^{(1,j)}) \leq d(v^{(1,i-1)}) \quad \text{for all} \quad j < i$$

and

$$d(v^{(1,l-1)}) < d(v^{(1,l)}) ,$$

thus

$$\begin{aligned} \sum_{j=l}^{i-1} (3d(v^{(1,j)}) - 1) &\leq \sum_{j=d(v^{(1,l)})}^{d(v^{(1,i-1)})} (3j - 1) \\ &= \frac{(3d(v^{(1,i-1)}) - 1 + 3d(v^{(1,l)}) - 1)(d(v^{(1,i-1)}) - d(v^{(1,l)}) + 1)}{2} \\ &= \frac{3d(v^{(1,i-1)})^2 + d(v^{(1,i-1)}) - 3d(v^{(1,l)})^2 + 5d(v^{(1,l)}) - 2}{2} . \end{aligned}$$

By the definition of i and l, it follows that

$$T_l \le 4d(v^{(1,l-1)}) + d(u) \ .$$

Since

$$d(v^{(1,l-1)}) \le d(v^{(1,l)}) - 1 \ ,$$

thus

$$\begin{aligned} T_i &\le d(u) + 4(d(v^{(1,l)}) - 1) \\ &\quad + \frac{3d(v^{(1,i-1)})^2 + d(v^{(1,i-1)}) - 3d(v^{(1,l)})^2 + 5d(v^{(1,l)}) - 2}{2} \\ &= d(u) + \frac{3d(v^{(1,i-1)})^2 + d(v^{(1,i-1)}) - 3d(v^{(1,l)})^2 + 13d(v^{(1,l)}) - 10}{2} \ . \end{aligned}$$

The right hand side of the inequality is a quadratic expression of $d(v^{(1,l)})$, having an absolute maximum at $d(v^{(1,l)}) = 2$, whence

$$T_i \le d(u) + (3d(v^{(1,i-1)})^2 + d(v^{(1,i-1)}) + 4)/2 \ . \tag{3.12}$$

If l with the above definition does not exist, then we have

$$T_i \le 1 + \frac{3d(v^{(1,i-1)})^2 + d(v^{(1,i-1)}) - 3d(v^{(1,l)})^2 + 5d(v^{(1,l)}) - 2}{2} \ ,$$

and (3.12) remains true.

For i we can define

$$u^{(1)} = v^{(1,i)} \ , \quad u^{(2)} = v^{(2,i)} \quad \text{and} \quad t = T_{i+1} - 1 \ .$$

If there are no i satisfying

$$\max\left\{T_{i-1} + 3d(v^{(1,i-1)}) - 1, 4d(v^{(1,i-1)}) + d(u)\right\} < T_i \ ,$$

then either

$$T(u) \le 5d(u)$$

or if

$$T_j > 4d(v^{(1,j)}) + d(u)$$

then

$$T_j \le T_{j-1} + 3dv^{(1,j-1)}) - 1 \quad \text{for all} \quad 1 < j \le m \ .$$

In both cases we may choose

$$u^{(1)} = u \ , \quad u^{(2)} = 0 \quad \text{and} \quad t = T(u) + 5d(u) \ . \quad \square$$

Remark 3.35. *The following problem is contained in a list of related questions in the paper of Tichy* [44].

Theorem 3.36. *Let $\pi \in \mathbb{N}$ be a prime, R be a Dedekind-domain, $P \in R$ be a prime ideal, such that $N(P) = \pi$, let $d \geq 2$ be an integer, u be a dth-order linear recurring sequence over R and let $S = \frac{3d^2+9d}{2} + 1$.*

If u is uniformly distributed modulo P^S, then it is also uniformly distributed modulo P^s for any $s \in \mathbb{N}$.

Proof. Suppose first that u is not purely periodic modulo P^s for some $s \geq 0$ and let $\varrho_s > 0$, such that

$$u_{\varrho_s+\varrho(u,s)+n} \equiv u_{\varrho_s+n} \mod P^s \quad \text{for every} \quad n \geq 0 \ .$$

Further, let $v_n^{(s)} = u_{\varrho_s+n}$. Clearly, $v^{(s)}$ is purely periodic modulo P^s and $v^{(s)}$ is u.d. modulo P^s if and only if u is u.d. modulo P^s. Thus, to prove that u is u.d. modulo P^s, it is enough to show that $v^{(s)}$ is u.d. modulo P^s.

Therefore, we may suppose without loss of generality, that for a fixed, but arbitrary big $s' \geq 0$, the sequence u is purely periodic modulo $P^{s'}$.

If $s \leq S$ then u is obviously u.d. modulo P^s. Suppose that $s \geq S$ and u is u.d. modulo P^s. By Lemma 3.34, u can be split into the sum of two linear recurring sequences,

$$u = u^{(1)} + u^{(2)} \quad \text{with} \quad u^{(2)} \equiv 0 \mod P^t \ ,$$

where

$$d(u^{(1)}) \leq d(u) \ ,$$

$$T(u^{(1)}) \leq \frac{3d(u^{(1)})^2 + d(u^{(1)})}{2} + 2 + d(u) \leq 3\frac{d(u)^2 + d(u)}{2} + 2$$

and

$$t > \max\left\{T(u^{(1)}) + 3d(u^{(1)}) - 1, 4d(u^{(1)}) + d(u)\right\} \ .$$

Hence

$$\begin{aligned} s \geq S &= \frac{3d(u)^2 + 9d(u)}{2} + 1 \\ &\geq \max\left\{3\frac{d(u)^2 + d(u)}{2} + 2 + 3d(u) - 1, 5d(u)\right\} \\ &\geq \max\left\{T(u^{(1)}) + 3d(u^{(1)}) - 1, 4d(u^{(1)}) + d(u)\right\} \ . \end{aligned}$$

Let

$$T' = \max\left\{d(u^{(2)}) + d(u^{(1)}), d(u^{(1)}) + T(u^{(1)}) - 1\right\} \ .$$

Since $u^{(2)}$ is a linear combination of u and $u^{(2)}$, by Lemma 3.8,

$$\begin{aligned} T' &= \max\left\{d(u^{(2)}) + d(u^{(1)}), d(u^{(1)}) + T(u^{(1)}) - 1\right\} \\ &\leq \max\left\{d(u) + 2d(u^{(1)}), d(u^{(1)}) + T(u^{(1)}) - 1\right\} \\ &< s \end{aligned}$$

thus u is u.d. modulo $P^{T'+1}$. Since $T' < t$, we have

$$u^{(1)} \equiv u \mod P^{T'+1}$$

and $u^{(1)}$ is u.d. modulo $P^{T'+1}$.

Hence, setting $k = d(u^{(1)})$, by Remark 3.29, we can choose $T_0 = T'$. Thus,

$$T_0 + 2d(u^{(1)}) \leq \max\left\{T(u^{(1)}) + 3d(u^{(1)}) - 1, 4d(u^{(1)}) + d(u)\right\} \leq s \ .$$

Similarly, $T_0 + 2d(u^{(1)}) \leq t$, whence by Corollary 3.33, $u = u^{(1)} + p^t u^{(2)}$ is u.d. modulo p^{s+1}.

Since s is arbitrary, we obtain the theorem by induction. □

Remark 3.37. *As we will see in Chapter 4, by a detailed analysis of the results in special cases we can obtain much better bounds than in the general case.*

For instance, if $T(u) = 1$, which is rather often the case for the uniform distribution property stated in Theorem 3.36, it is enough if

$$s \geq 3d(u) + 1 \ .$$

Chapter 4

Construction of uniformly distributed linear recurring sequences

In this chapter, we will provide the theoretical background for construction of uniformly distributed linear recurring sequences with arbitrary large period length using the general results of the previous chapter. The fundamental application of such sequences is the construction of pseudo-random number generators.

If we want to use a periodic sequence u for pseudo-random number generation, we have to care to the followings:

The sequence u should
- be uniformly distributed
- have a long minimal period
- have a low correlation between the elements
- be easily computable.

We will provide a solution for the problem paying particular attention to the above mentioned properties.

Remark 4.1. *One can find criteria for the uniform distribution of linear recurring sequences of order* ≤ 4 *over finite fields in* [31] *and* [32].

Among other general results, criteria for the uniform distribution of linear recurring sequences of order ≤ 3 *over Dedekind-domains can be find in* [46] *and* [47].

As a starting point we have to construct uniformly distributed recurring sequences over simpler structures. Niederreiter and Shiue in [31] give a necessary condition on uniform distribution of linear recurring sequences over finite fields:

Proposition 4.2. *Let* F *be a finite field and let* u *be a l.r.s. over* F. *If* u *is uniformly distributed, the characteristic polynomial of* u *contains a multiple factor.*

Proof. See e.g. [31]. □

Example 4.3. *Let us define the sequence* u *by the following:*

$$u_0 = 0\ , \quad u_1 = 1 \quad \textit{and} \quad u_n = u_{n-2} \quad \textit{for} \quad n \geq 2\ .$$

Clearly, the sequence is uniformly distributed modulo 2. *The characteristic polynomial of* u *is*

$$P(x) = x^2 - 1 \equiv (x+1)^2 \mod 2\ .$$

Example 4.4. *Define the sequence u by the following:*

$$u_0 = 0\ , \quad u_1 = 1 \quad \textit{and} \quad u_n = u_{n-1} + u_{n-2} \quad \textit{for} \quad n \geq 2\ .$$

The sequence u is the so-called Fibonacci-sequence. In [29] *it is proven that u is uniformly distributed modulo* 5*. Even more proven there: u is uniformly distributed modulo m if and only if m is a power of* 5*.*

The characteristic polynomial of u is

$$P(x) = x^2 - x - 1 \equiv (x+2)^2 \mod 5\ .$$

Now we turn to the known and the new results which we will use for finding linear recurring sequences with uniform distribution modulo some - in particular 2^k - integer. The idea behind the construction is that first we try to find a linear recurring sequence with a characteristic polynomial having the property

$$P(x) \equiv (x+1)^2 Q(x) \mod 2\ ,$$

where $Q(x)$ is irreducible modulo 2 and has a particular degree. In this way we can find a linear recurring sequence with a large period length, which has some advantages for the later steps.

Definition 4.5. *Let F be a finite field and $P \in F[x]$, such that $P(0) \neq 0$. We will call $ord(P) = e$ the* **order** *of P, where e is the smallest positive integer, such that $P(x) \mid x^e - 1$ over $F[x]$.*

Remark 4.6. *The integer e in the above definition always exists. See e.g. in* [24]

Proposition 4.7. *Let F be a finite field with q elements and let $Q(x)$ be an irreducible polynomial of degree k over F. Then the order of Q divides $q^k - 1$.*

Proof. See e.g. Corollary 3.4 of [24]. □

Proposition 4.8. *Let F be a finite field of characteristic p, let $P \in F[x]$ be a polynomial of positive degree with $P(0) \neq 0$ and let $P = aP_1^{b_1} \dots P_r^{b_r}$, where $a \in F$ and $P_1, \dots, P_r$ are distinct monic irreducible polynomials.*

If e denotes the least common multiple of $ord(P_1), \dots, ord(P_r)$ and t denotes the smallest integer, such that $p^t \geq \max\{b_1, \dots, b_r\}$, then $ord(P) = ep^t$.

Proof. See e.g. Theorem 3.11 of [24]. □

We can use the above result to determine the order of polynomials in the demanded form.

Corollary 4.9. *Let $P(x) \in \mathbb{Z}[x]$ be such that*

$$P(x) \equiv (x+1)^2 Q(x) \mod 2\ ,$$

where $Q(x)$ is irreducible modulo 2*.*

Then for the orders of the polynomials over $\mathbb{F}_2$ we have

$$ord(P) = 2ord(Q)\ .$$

Definition 4.10. *Let u be a l.r.s. of order d over a Dedekind-domain R. We say that u is an* **impulse response sequence** *if*

$$u_0 = \cdots = u_{d-2} = 0 \quad \textit{and} \quad u_{d-1} = 1 \ .$$

The following proposition shows the highlighted role of the impulse response sequence corresponding to a given recurrence relation.

Proposition 4.11. *Let F be a finite field and let u be the impulse response sequence over F with characteristic polynomial $P(x)$. Then the minimal period length of u is equal to $ord(P)$.*

Proof. See e.g. Theorem 6.27. of [24]. □

Definition 4.12. *Let $m > 1$ be an integer, let u_n be a sequence of integers and let $u'_n \in \{0, \ldots, m-1\}$ be such that*

$$u'_n \equiv u_n \mod m \ .$$

The sequence u' is called the **reduced sequence** *of u mod m.*

The following lemma provides the possibility to construct linear recurring sequences with large period lengths.

Lemma 4.13. *Let $Q(x) \in \mathbb{Z}[x]$ be an irreducible polynomial modulo 2 of degree k and let u be the impulse response sequence corresponding to the characteristic polynomial $P(x) \equiv (x^2-1)Q(x) \mod 2$. Then u' – the reduced sequence of u modulo 2 – has period length 2ϱ with some ϱ, such that $\varrho \mid 2^k - 1$.*

Proof. Let $\varrho = ord(Q)$. By Proposition 4.7, $\varrho \mid 2^k - 1$. The factorization of P is $P \equiv (x+1)^2 Q(x) \mod 2$, whence by Corollary 4.9,

$$\operatorname{ord}(P) = 2 \operatorname{ord}(Q) = 2\varrho \ .$$

Hence by Proposition 4.11, the lemma follows. □

Lemma 4.14. *Let $Q(x) \in \mathbb{Z}[x]$, such that $2 \nmid Q(1)$ and let u be a l.r.s. of integers with characteristic polynomial*

$$P(x) \equiv (x^2-1)Q(x) \mod 2 \ ,$$

let v be the sequence given by

$$v_n = u_n + 1 \quad \textit{for all} \quad n \geq 0$$

and let v' denote the modulo 2 reduced sequence of v. Then v' modulo 2 satisfies the recurrence relation corresponding to P.

Proof. The polynomial P is a characteristic polynomial of the sequence w modulo 2, where $w_n = 1$ for all $n \geq 0$, whence by the additive property of linear recurring sequences, the lemma follows. □

Remark 4.15. *The above lemma is proven in more general settings in Theorem 6.62 of* [24].

Definition 4.16. *Let F be a finite field with q elements and let u and v be two linear recurring sequences of order d with the same characteristic polynomial P. Suppose that $P(0) \neq 0$. We will say that u and v are* **equivalent**, *if there exists $N \in \mathbb{N}$, such that*

$$u_n = v_{n+N} \quad \textit{for all} \quad n \in \mathbb{N}$$
$$\textit{or}$$
$$u_{n+N} = v_n \quad \textit{for all} \quad n \in \mathbb{N} \ .$$

Remark 4.17. *The following properties are easy to prove. Let F be a finite field with q elements and let $P \in F[x]$ be a polynomial of degree d. Then*

i) we have q^d different linear recurring sequences having characteristic polynomial P, and they can be divided into equivalence classes, such that
ii) in every equivalence class, the sequences have the same minimal period length
iii) the cardinality of the equivalence classes are equal to its elements' common minimal period length
iv) the sequences from the same equivalence classes have periods differing only in cyclic permutations.

Lemma 4.18. *Let $Q(x) \in \mathbb{Z}[x]$ be irreducible modulo 2 of degree k and let*

$$P(x) \equiv (x+1)^2 Q(x) \mod 2 \ .$$

Let u be a sequence having characteristic polynomial P and minimal period length modulo 2 equal to ord(P). Then u is uniformly distributed modulo 2.

Proof. Let denote by L the different linear recurring sequences having characteristic polynomial P modulo 2. (We will regard two linear recurring sequences the same modulo 2 if their reduced sequences are the same.) By (i) of Remark 4.17 , $\#(L) = 2^{k+2}$. We will use the fact that if Q is a characteristic polynomial of a l.r.s., then $Q \cdot Q'$ is also a characteristic polynomial of it, for all Q' non-zero monic polynomials. We can partition $L = L_1 \cup L_2$, such that $\#(L_1) = \#(L_2) = 2^{k+1}$ by the following: a l.r.s. is in L_1 if it satisfies the recurrence relation corresponding to the characteristic polynomial $(x+1)Q(x) \mod 2$ and it is in L_2 otherwise. There is a simple bijection between L_1 and L_2, given by the mapping $\varphi : L \to L$, where $\varphi(w) = v$, such that $v_i = w_i$ for $i = 0, \ldots, k$ and $v_{k+1} = 1 + w_{k+1}$. Clearly $\varphi^2 = Id$ and $\varphi(L_1) = L_2$. One can easily check the following interesting property of φ. Namely, for any two sequences $v, w \in L$,

$$w + v \equiv \varphi(w) + \varphi(v) \mod 2 \ .$$

By the definition of L_1, if $w, v \in L_1$, then $w + v \in L_1$, too. Further if $w, v \in L_2$, then $\varphi(w), \varphi(v) \in L_1$, whence $w + v \in L_1$.

Let v be a l.r.s., we will use the notation $\bar{v}_n = (v_n, \ldots, v_{n+k+1})$ for the $k+2$ dimensional state vector of v.

Let $\varrho = \mathrm{ord}(Q)$. Then $\mathrm{ord}((x+1)Q) = \varrho$ and $\mathrm{ord}(P) = 2\varrho$.

By the definition of u we know that $u \in L_2$ and in other words,

$$\bar{u}_0 \equiv \bar{u}_{2\varrho} \mod 2$$
and
$$\bar{u}_0 \not\equiv \bar{u}_{\varrho} \mod 2 .$$

Let $w \in L$ be the sequence, for which

$$\bar{w}_0 \equiv \bar{u}_{\varrho} - \bar{u}_0 \mod 2 .$$

Clearly

$$\bar{u}_{n+\varrho} \equiv \bar{u}_n + \bar{w}_n \mod 2 \text{ for all } n \in \mathbb{N} .$$

Let v be the sequence, for which

$$\bar{v}_0 \equiv \bar{u}_1 \mod 2 .$$

Since $u, v \in L_2$ thus $u + v \in L_1$ and

$$\bar{u}_{\varrho} + \bar{v}_{\varrho} \equiv \bar{u}_0 + \bar{v}_0 \mod 2 ,$$

i.e.

$$\bar{u}_{\varrho} + \bar{u}_{\varrho+1} \equiv \bar{u}_0 + \bar{u}_1 \mod 2 .$$

This means that

$$\bar{u}_0 + \bar{w}_0 + \bar{u}_1 + \bar{w}_1 \equiv \bar{u}_0 + \bar{u}_1 \mod 2 ,$$

i.e.

$$\bar{w}_0 \equiv \bar{w}_1 \mod 2 .$$

Since $w \not\equiv 0 \mod 2$ this yields that $w_n \equiv 1 \mod 2$ for all $n \in \mathbb{N}$.

Consequently

$$u_n \equiv u_{n+\varrho} + 1 \mod 2 \qquad \text{for all } n \in \mathbb{N} . \tag{4.1}$$

But this means that the number of 0s among the first ϱ elements of the sequence is equal to the number of 1s among the second ϱ elements of the sequence and vice versa. Then the number of 0s and 1s has to be the same in a period, which means that u is uniformly distributed modulo 2. □

Remark 4.19. *The statement of the theorem is proven in more general settings in* [31].

Theorem 4.20. *Let $Q \in \mathbb{Z}[x]$ be monic and irreducible modulo 2 with degree k and let $P \in \mathbb{Z}[x]$ be monic and such that*

$$P(x) \equiv (x^2 - 1)Q(x) \mod 2 .$$

Let us define

$$P_1(x) = P(x) ,$$
$$P_2(x) = P(x) - 2 ,$$
$$P_3(x) = P(x) - 2x ,$$
$$P_4(x) = P(x) - 2x - 2$$

and let $u^{(i)}$ be linear recurring sequences corresponding to P_i, such that the minimal period length of $u^{(i)}$ modulo 2 is $2ord(Q)$, where $ord(Q)$ is the order in $\mathbb{F}_2[x]$. Then at least one of the $u^{(i)}$'s is uniformly distributed modulo 2^s with period length $2^s ord(Q)$ for any $s \in \mathbb{N}$.

Proof. Simplifying the proof, we suppose, that

$$\bar{u}_0^{(1)} = \bar{u}_0^{(2)} = \bar{u}_0^{(3)} = \bar{u}_0^{(4)} \ ,$$

where $\bar{u}_n$ is the state vector of u_n. In the proof we will use the notation $\varrho = \mathrm{ord}(Q)$ and $M_{(i)}$ for the companion matrix. Furthermore, in any case we will use upper or lower index (i) with the different symbols corresponding to the proper sequence for $i = 1, 2, 3, 4$. For short, we will write $u = u^{(1)}$. For the convenient reference and better overview, we will enumerate the parts of the proof.

(i) Let us calculate

$$\bar{u}_{2\varrho+n} - \bar{u}_n = M^{2\varrho}\bar{u}_n - \bar{u}_n = (M^{2\varrho} - E)\bar{u}_n = (M^{\varrho} + E)(M^{\varrho} - E)\bar{u}_n \ , \tag{4.2}$$

where M is the companion matrix of u and E is the unit matrix of the same dimension. As we have seen in Lemma 4.18, by (4.1) we know, that

$$(M^{\varrho} - E)\bar{u}_n = \bar{1} + 2\bar{y}_n \ ,$$

with some $\bar{y}_n$. Here $\bar{1}$ yields the $k+2$ dimensional $(1, 1, \ldots, 1)$ vector. One should remark, that the equation $\bar{y}_{n+1} = M\bar{y}_n$ not necessarily holds.

(ii) For the further calculations, examine first the behaviour of $M^{\varrho}\bar{1}$. Since the sequence $1, 1, 1 \ldots$ satisfies the recurrence relation with characteristic polynomial $x - 1$ and $x - 1$ divides $P_1(x)$, $P_2(x)$, $P_3(x)$ and $P_4(x)$ modulo 2, thus $1, 1, 1 \ldots$ also satisfies the recurrence relations with characteristic polynomials $P_1(x)$, $P_2(x)$, $P_3(x)$ and $P_4(x)$ modulo 2. Consequently

$$M\bar{1} = \bar{1} + 2\bar{v} \ \text{ and } \ M^{\varrho}\bar{1} = \bar{1} + 2\bar{z} \ ,$$

with some $\bar{v}$ and $\bar{z}$.

Clearly, either $\bar{v} \equiv \bar{0} \mod 2$ or $\bar{v} \equiv (0, 0, \ldots, 0, 1) \mod 2$. We will use the notation $\bar{e} = (0, 0, \ldots, 0, 1) = \bar{u}_0$. In the first case, $\bar{z} \equiv \bar{0} \mod 2$ should hold, too. In the second case

$$M^{\varrho+1}\bar{1} = M^{\varrho}(\bar{1} + 2\bar{v}) = \bar{1} + 2\bar{z} + 2M^{\varrho}\bar{v} \equiv \bar{1} + 2\bar{z} + 2M^{\varrho}\bar{u}_0 = \\ \bar{1} + 2\bar{z} + 2(\bar{1} + \bar{e} + 2\bar{y}_0) \equiv \bar{1} + 2(\bar{z} + \bar{1} + \bar{e}) \mod 4 \ .$$

Let $\bar{z} = (z_1, z_2, \ldots, z_{k+2})$. Then

$$(\bar{z} + \bar{1} + \bar{e}) \equiv (z_2, \ldots, z_{k+2}, z') \mod 2$$

with some $z' \in \mathbb{Z}$. But this yields that

$$\begin{aligned} z_1 &\equiv z_2 + 1 \mod 2 \\ z_2 &\equiv z_3 + 1 \mod 2 \\ &\ldots \\ z_{k+1} &\equiv z_{k+2} + 1 \mod 2 \ , \end{aligned}$$

i.e. $\bar{z}$ is congruent to one of the alternating vectors beginning with $(0,1,0,1,\dots)$ or $(1,0,1,0,\dots)$ modulo 2.

(iii) We may write $M_{(i)}\bar{1} = \bar{1} + 2\bar{v}^{(i)}$ corresponding to the different recurrence relations for $i = 1,2,3,4$. By the above, if $\bar{z}^{(1)} \equiv \bar{0} \mod 2$, then $\bar{v}^{(1)} \equiv \bar{0} \mod 2$. Hence by the properties of $P_1(x)$, $P_2(x)$, $P_3(x)$ and $P_4(x)$ we have

$$\bar{v}^{(2)} \equiv \bar{v}^{(3)} \equiv \bar{e} \mod 2 \quad \text{and} \quad \bar{v}^{(4)} \equiv \bar{0} \mod 2$$

which yield that $\bar{z}^{(2)}$ and $\bar{z}^{(3)}$ are congruent to some of the vectors $(0,1,0,1,\dots)$ and $(1,0,1,0,\dots)$ modulo 2 and $\bar{z}^{(4)} \equiv \bar{0} \mod 2$. Similarly, if $\bar{z}^{(1)}$ is congruent to one of $(0,1,0,1,\dots)$ and $(1,0,1,0,\dots)$ modulo 2, then $\bar{v}^{(1)} \equiv \bar{u}_0 \mod 2$, whence

$$\bar{v}^{(2)} \equiv \bar{v}^{(3)} \equiv \bar{0} \mod 2 \quad \text{and} \quad \bar{v}^{(4)} \equiv \bar{e} \mod 2\ ,$$

i.e.

$$\bar{z}^{(2)} \equiv \bar{z}^{(3)} \equiv \bar{0} \mod 2$$

and $\bar{z}^{(4)}$ is congruent to one of $(0,1,0,1,\dots)$ and $(1,0,1,0,\dots)$ modulo 2.

(iv) Now, examine the behaviour of $M^{\varrho}\bar{y}_n$. Since $\bar{u}_0, \bar{u}_1, \dots, \bar{u}_{k+1}$ are independent modulo 2, they form a basis in $\mathbb{Z}_2^{k+2}$ and there exist $\alpha_0, \alpha_1, \dots, \alpha_{k+1} \in \mathbb{Z}$ such that

$$\bar{y}_n \equiv \alpha_0\bar{u}_0 + \alpha_1\bar{u}_1 + \dots + \alpha_{k+1}\bar{u}_{k+1} \mod 2\ .$$

Hence. by (4.1)

$$\begin{aligned} M^{\varrho}\bar{y}_n &\equiv M^{\varrho}(\alpha_0\bar{u}_0 + \alpha_1\bar{u}_1 + \dots + \alpha_{k+1}\bar{u}_{k+1}) \\ &\equiv M^{\varrho}\alpha_0\bar{u}_0 + M^{\varrho}\alpha_1\bar{u}_1 + \dots + M^{\varrho}\alpha_{k+1}\bar{u}_{k+1} \\ &\equiv \alpha_0 M^{\varrho}\bar{u}_0 + \alpha_1 M^{\varrho}\bar{u}_1 + \dots + \alpha_{k+1}M^{\varrho}\bar{u}_{k+1} \\ &\equiv \alpha_0(\bar{1} + \bar{u}_0) + \alpha_1(\bar{1} + \bar{u}_1) + \dots + \alpha_{k+1}(\bar{1} + \bar{u}_{k+1}) \\ &\equiv (\alpha_0 + \alpha_1 + \dots + \alpha_{k+1}) \cdot \bar{1} + \bar{y}_n \\ &\equiv \delta_n \cdot \bar{1} + \bar{y}_n \mod 2\ , \end{aligned}$$

with some $\delta_n \in \{0,1\}$.

(v) Now, by (4.2) we can write

$$\begin{aligned} \bar{u}_{2\varrho+n} - \bar{u}_n &= (M^{\varrho} + E)(M^{\varrho} - E)\bar{u}_n \\ &= (M^{\varrho} + E)(\bar{1} + 2\bar{y}_n) \\ &= \bar{1} + 2\bar{z} + \bar{1} + 2M^{\varrho}\bar{y}_n + 2\bar{y}_n \\ &\equiv 2(\bar{1} + \bar{z}) + 2(\delta\bar{1} + \bar{y}_n) + 2\bar{y}_n \\ &\equiv 2(\bar{1} + \bar{z} + \delta_n\bar{1} + 2\bar{y}_n) \\ &\equiv 2(\bar{1} + \bar{z} + \delta_n\bar{1}) \mod 4\ . \end{aligned} \tag{4.3}$$

Similarly,

$$\bar{u}_{2\varrho+n+1} - \bar{u}_{n+1} \equiv 2(\bar{1} + \bar{z} + \delta_{n+1}\bar{1}) \mod 4\ . \tag{4.4}$$

Assume that

$$\bar{u}_{2\varrho+n} - \bar{u}_n = (w_n, w_{n+1}, \dots, w_{n+k+1}) \tag{4.5}$$

and

$$\bar{u}_{2\varrho+n+1} - \bar{u}_{n+1} = (w_{n+1}, w_{n+2}, \dots, w_{n+k+2}) \ . \tag{4.6}$$

Then by (4.3) and (4.5)

$$\begin{aligned} w_n &\equiv 2(1 + z_1 + \delta_n) \mod 4 \\ w_{n+1} &\equiv 2(1 + z_2 + \delta_n) \mod 4 \\ &\dots \\ w_{n+k+1} &\equiv 2(1 + z_{k+2} + \delta_n) \mod 4 \end{aligned}$$

and by (4.4) and (4.6)

$$\begin{aligned} w_{n+1} &\equiv 2(1 + z_1 + \delta_{n+1}) \mod 4 \\ w_{n+2} &\equiv 2(1 + z_2 + \delta_{n+1}) \mod 4 \\ &\dots \\ w_{n+k+2} &\equiv 2(1 + z_{k+2} + \delta_{n+1}) \mod 4 \ . \end{aligned}$$

This yields that

if $\bar{z} \equiv (0, 0, \dots, 0) \mod 2$ then $\delta_n = \delta_{n+1}$ and

if $\bar{z}$ is congruent to one of $(0, 1, \dots)$ or $(1, 0, \dots)$ then $\delta_n = 1 - \delta_{n+1}$.

(vi) In the following we will prove that $\bar{z}^{(i)} \equiv \bar{0} \mod 2$ and $\delta_0^{(i)} = 0$ for at least one of the $i = 1, 2, 3, 4$. (If $\bar{z}^{(i)} \equiv \bar{0} \mod 2$ and $\delta_0^{(i)} = 0$, then $\delta_n^{(i)} = 0$ for all $n \in \mathbb{N}$.)

Suppose, that $\bar{z}^{(1)} \not\equiv \bar{0} \mod 2$ or $\delta_0^{(1)} \neq 0$.

(vi.a) Clearly, $u_n^{(i)} \equiv u_n^{(j)} \mod 2$ for any $i, j = 1, 2, 3, 4$. Define the sequences $r_n^{(i)}$ by $u_n^{(i)} = u_n^{(1)} + 2r_n^{(i)}$ for $i = 2, 3, 4$ and denote $\hat{u}_n = (0, 0, \dots, 0, u_n) \in \mathbb{Z}^{k+2}$.

By the definition of $M_{(i)}$,

$$\bar{u}_{n+1}^{(2)} = M_{(2)}\bar{u}_n^{(2)} = M_{(1)}\bar{u}_n^{(2)} + 2\hat{u}_n^{(2)} \ ,$$

$$\bar{u}_{n+1}^{(3)} = M_{(3)}\bar{u}_n^{(3)} = M_{(1)}\bar{u}_n^{(3)} + 2\hat{u}_{n+1}^{(3)}$$

and

$$\bar{u}_{n+1}^{(4)} = M_{(4)}\bar{u}_n^{(4)} = M_{(1)}\bar{u}_n^{(4)} + 2(\hat{u}_n^{(4)} + \hat{u}_{n+1}^{(4)})$$

for all $n \geq 0$.

Hence

$$\begin{aligned} \bar{u}_{n+1}^{(1)} + 2\bar{r}_{n+1}^{(2)} &= \bar{u}_{n+1}^{(2)} \\ &= M_{(1)}(\bar{u}_n^{(1)} + 2\bar{r}_n^{(2)}) + 2(\hat{u}_n^{(1)} + 2\hat{r}_n^{(2)}) \\ &= \bar{u}_{n+1}^{(1)} + 2(M_{(1)}\bar{r}_n^{(2)} + \hat{u}_n^{(1)} + 2\hat{r}_n^{(2)}) \ , \end{aligned}$$

$$\begin{aligned}\bar{u}_{n+1}^{(1)} + 2\bar{r}_{n+1}^{(3)} &= \bar{u}_{n+1}^{(3)} \\ &= M_{(1)}(\bar{u}_n^{(1)} + 2\bar{r}_n^{(3)}) + 2(\hat{u}_{n+1}^{(1)} + 2\hat{r}_{n+1}^{(3)}) \\ &= \bar{u}_{n+1}^{(1)} + 2(M_{(1)}\bar{r}_n^{(3)} + \hat{u}_{n+1}^{(1)} + 2\hat{r}_{n+1}^{(3)})\end{aligned}$$

and

$$\begin{aligned}\bar{u}_{n+1}^{(1)} + 2\bar{r}_{n+1}^{(4)} &= \bar{u}_{n+1}^{(4)} \\ &= M_{(1)}(\bar{u}_n^{(1)} + 2\bar{r}_n^{(4)}) + 2(\hat{u}_n^{(1)} + \hat{u}_{n+1}^{(1)} + 2(\hat{r}_n^{(4)} + \hat{r}_{n+1}^{(4)})) \\ &= \bar{u}_{n+1}^{(1)} + 2(M_{(1)}\bar{r}_n^{(4)} + \hat{u}_n^{(1)} + \hat{u}_{n+1}^{(1)} + 2(\hat{r}_n^{(4)} + \hat{r}_{n+1}^{(4)}))\ .\end{aligned}$$

Subtracting $\bar{u}_{n+1}^{(1)}$ and cancelling out 2, we obtain

$$\begin{aligned}&\bar{r}_{n+1}^{(2)} = M_{(1)}\bar{r}_n^{(2)} + \hat{u}_n^{(1)} + 2\hat{r}_n^{(2)}\ , \\ &\bar{r}_{n+1}^{(3)} = M_{(1)}\bar{r}_n^{(3)} + \hat{u}_{n+1}^{(1)} + 2\hat{r}_{n+1}^{(3)} \\ &\qquad \text{and} \\ &\bar{r}_{n+1}^{(4)} = M_{(1)}\bar{r}_n^{(4)} + \hat{u}_n^{(1)} + \hat{u}_{n+1}^{(1)} + 2(\hat{r}_n^{(4)} + \hat{r}_{n+1}^{(4)})\end{aligned} \tag{4.7}$$

for all $n \geq 0$. Further $\bar{r}_0^{(i)} = \bar{0}$ for $i = 2, 3, 4$.

(vi.b) One can prove

$$\bar{r}_{n+1}^{(2)} \equiv \bar{r}_n^{(3)} + M_{(1)}^n \hat{u}_0^{(1)} \mod 2 \quad \text{for all } n \geq 0 \tag{4.8}$$

by the following:

Since $u_0 = 0$, thus in the case $n = 0$ by (4.7)

$$\bar{r}_1^{(2)} = M_{(1)}\bar{r}_0^{(2)} + \hat{u}_0^{(1)} + 2\hat{r}_0^{(2)} \equiv M_{(1)}\bar{0} + \hat{u}_0^{(1)} = \bar{0} + \hat{u}_0^{(1)} = \bar{r}_0^{(3)} + \hat{u}_0^{(1)} \mod 2\ .$$

Suppose that

$$\bar{r}_{n+1}^{(2)} \equiv \bar{r}_n^{(3)} + M_{(1)}^n \hat{u}_0^{(1)} \mod 2 \quad \text{for some } n \geq 0\ .$$

Then again by (4.7)

$$\begin{aligned}\bar{r}_{n+2}^{(2)} &= M_{(1)}\bar{r}_{n+1}^{(2)} + \hat{u}_{n+1}^{(1)} + 2\hat{r}_{n+1}^{(2)} \\ &\equiv M_{(1)}(\bar{r}_n^{(3)} + M_{(1)}^n \hat{u}_0^{(1)}) + \hat{u}_{n+1}^{(1)} \\ &\equiv \bar{r}_{n+1}^{(3)} + M_{(1)}^{n+1}\hat{u}_0^{(1)} \qquad \mod 2\ .\end{aligned}$$

Hence by induction, the aim follows.

Similarly one can prove that

$$\bar{r}_n^{(4)} \equiv \bar{r}_n^{(2)} + \bar{r}_n^{(3)} \mod 2 \quad \text{for all } n \geq 0\ . \tag{4.9}$$

(vi.c) By (4.3) we can write

$$\bar{u}_{2\varrho}^{(1)} + 2\bar{r}_{2\varrho}^{(i)} - (\bar{u}_0^{(1)} + 2\bar{r}_0^{(i)}) = \bar{u}_{2\varrho}^{(i)} - \bar{u}_0^{(i)} \equiv 2(\bar{1} + \bar{z}^{(i)} + \delta_0^{(i)}\bar{1}) \mod 4$$

for all $i = 2, 3, 4$. Again by (4.3), using that $\bar{r}_0^{(i)} = \bar{0}$,

$$2(\bar{1} + \bar{z}^{(1)} + \delta_0^{(1)}\bar{1}) + 2\bar{r}_{2\varrho}^{(i)} \equiv 2(\bar{1} + \bar{z}^{(i)} + \delta_0^{(i)}\bar{1}) \mod 4 ,$$

which is equivalent to

$$\bar{z}^{(1)} + \delta_0^{(1)}\bar{1} + \bar{r}_{2\varrho}^{(i)} \equiv \bar{z}^{(i)} + \delta_0^{(i)}\bar{1} \mod 2 \tag{4.10}$$

for all $i = 2, 3, 4$.

(vi.d) At the beginning of part (vi) we assumed that $\bar{z}^{(1)} \not\equiv \bar{0} \mod 2$ or $\delta_0^{(1)} \neq 0$. Suppose first that $\bar{z}^{(1)} \not\equiv \bar{0} \mod 2$. By part (iii) of the proof, we have then $\bar{z}^{(i)} \equiv \bar{0} \mod 2$ for $i = 2, 3$. Assume further that $\delta_0^{(2)} \neq 0$. (i.e. $\delta_0^{(2)} = 1$).

By (4.10)

$$\bar{r}_{2\varrho}^{(i)} \equiv \bar{z}^{(1)} + \delta_0^{(1)}\bar{1} + \delta_0^{(i)}\bar{1} \mod 2$$

for $i = 2, 3$. Since by part (ii) $\bar{z}^{(1)}$ is congruent to one of $(0, 1, 0, 1, \dots)$ and $(1, 0, 1, 0, \dots)$ modulo 2, thus $\bar{r}_{2\varrho}^{(2)}$ and $\bar{r}_{2\varrho}^{(3)}$ are also congruent to some of the vectors $(0, 1, 0, 1, \dots)$ and $(1, 0, 1, 0, \dots)$ modulo 2. But by (4.8)

$$\bar{r}_{2\varrho+1}^{(2)} \equiv \bar{r}_{2\varrho}^{(3)} + M_{(1)}^{2\varrho}\hat{u}_0 \equiv \bar{r}_{2\varrho}^{(3)} + \hat{u}_0 \mod 2 ,$$

whence if

$$\bar{r}_{2\varrho}^{(2)} \equiv (0, 1, 0, 1, \dots) \mod 2 ,$$

then

$$\bar{r}_{2\varrho}^{(3)} \equiv (1, 0, 1, 0, \dots) \mod 2 ,$$

and vice versa. Hence, by (4.10)

$$\delta_0^{(3)}\bar{1} \equiv \bar{r}_{2\varrho}^{(2)} + \bar{r}_{2\varrho}^{(3)} + \delta_0^{(2)}\bar{1} \equiv \bar{1} + \bar{1} \equiv \bar{0} \mod 2 ,$$

that is both condition $\bar{z}^{(3)} \equiv \bar{0} \mod 2$ and $\delta_0^{(3)} = 0$ are fulfilled.

Suppose now that $\bar{z}^{(1)} \equiv \bar{0} \mod 2$. Then, by part (iii) of the proof, we have $\bar{z}^{(4)} \equiv \bar{0} \mod 2$. Since we assumed at the beginning of this part that $\bar{z}^{(1)} \equiv \bar{0} \mod 2$ and $\delta^{(1)} = 0$ do not hold simultaneously, we have $\delta^{(1)} = 1$. By (4.10) we can write

$$\bar{z}^{(1)} + \delta_0^{(1)}\bar{1} + \bar{r}_{2\varrho}^{(4)} \equiv \bar{z}^{(4)} + \delta_0^{(4)}\bar{1} \mod 2 .$$

By (4.9)

$$\bar{z}^{(1)} + \delta_0^{(1)}\bar{1} + \bar{r}_{2\varrho}^{(2)} + \bar{r}_{2\varrho}^{(3)} \equiv \bar{z}^{(4)} + \delta_0^{(4)}\bar{1} \mod 2 .$$

Similarly as above we can prove that

$$\bar{r}_{2\varrho}^{(2)} + \bar{r}_{2\varrho}^{(3)} \equiv \bar{1} \mod 2 ,$$

whence substituting the proper values for $\bar{z}^{(1)}$, $\bar{z}^{(4)}$ and $\delta_0^{(1)}$ we obtain

$$\bar{1} + \bar{1} \equiv \delta_0^{(4)}\bar{1} \mod 2 .$$

But this yields that $\bar{z}^{(4)} \equiv \bar{0} \mod 2$ and $\delta_0^{(4)} = 0$.

With this we could prove the aim of part (vi). We should remark here, that the careful reading of the proof gives a stronger result, namely that $\bar{z}^{(i)} \equiv \bar{0} \mod 2$ and $\delta_0^{(i)} = 0$ hold simultaneously for exactly one $i \in \{1, 2, 3, 4\}$.

(vii) In the followings there are of no account for which i the above proven condition holds, so for simplification of writing, we suppose, that $i = 1$.

In this part of the proof we will prove that

$$u_{2^s\varrho+n} \equiv u_n + 2^s \mod 2^{s+1} \tag{4.11}$$

for all $s = 1, 2, \ldots$ and $n = 0, 1, \ldots$.

(vii.a) We know that

$$M^{2\varrho}\bar{y} \equiv \bar{y} \mod 2 \qquad \text{for all } \bar{y} \in \mathbb{Z}^{k+2} .$$

Suppose that for a fixed s

$$M^{2^s\varrho}\bar{y} \equiv \bar{y} \mod 2^s \qquad \text{for all } \bar{y} \in \mathbb{Z}^{k+2}$$

holds. Then

$$\begin{aligned} M^{2^{s+1}\varrho}\bar{y} - \bar{y} &= (M^{2^{s+1}\varrho} - E)\bar{y} \\ &= (M^{2^s\varrho} + E)(M^{2^s\varrho} - E)\bar{y} \\ &\equiv (M^{2^s\varrho} + E)2^s\bar{x} \\ &\equiv M^{2^s\varrho}2^s\bar{x} + 2^s\bar{x} \\ &\equiv 2^{s+1}\bar{x} \\ &\equiv \bar{0} \qquad \mod 2^{s+1} \end{aligned}$$

with some $\bar{x} \in \mathbb{Z}^{k+2}$ for any $\bar{y} \in \mathbb{Z}^{k+2}$. This yields that

$$M^{2^s\varrho}\bar{y} \equiv \bar{y} \mod 2^s \tag{4.12}$$

for any $\bar{y} \in \mathbb{Z}^{k+2}$ and $s = 1, 2, \ldots$.

(vii.b) Recall that in our case $\bar{z} \equiv \bar{0} \mod 2$, whence

$$M^{2\varrho}\bar{1} \equiv \bar{1} \mod 4 .$$

Suppose that for a fixed s

$$M^{2^s\varrho}\bar{1} \equiv \bar{1} \mod 2^{s+1} .$$

Then by (4.12)

$$\begin{aligned} M^{2^{s+1}\varrho}\bar{1} &= M^{2^s\varrho}M^{2^s\varrho}\bar{1} \\ &\equiv M^{2^s\varrho}(\bar{1}+2^{s+1}\bar{y}_n) \\ &\equiv M^{2^s\varrho}\bar{1}+M^{2^s\varrho}2^{s+1}\bar{y}_n \\ &\equiv \bar{1}+2^{s+1}\bar{y}_n+2^{s+1}\bar{y}_n \\ &\equiv \bar{1} \mod 2^{s+2} \end{aligned}$$

with some $\bar{y}_n \in \mathbb{Z}^{k+2}$. This yields that

$$M^{2^s\varrho}\bar{1} \equiv \bar{1} \mod 2^{s+1} \tag{4.13}$$

for all $s = 1, 2, \ldots$.

(vii.c) By (4.3)

$$\bar{u}_{2\varrho+n} - \bar{u}_n \equiv 2(\bar{1}+\bar{z}+\delta_n\bar{1}) \equiv 2\cdot\bar{1} \mod 4\ .$$

This means that

$$u_{2\varrho+n} \equiv u_n + 2 \mod 4 \qquad \text{for all } n \in \mathbb{N}\ .$$

Suppose, that s is fixed and

$$u_{2^s\varrho+n} \equiv u_n + 2^s \mod 2^{s+1} \qquad \text{for all } n = 0, 1, \ldots\ .$$

Then by (4.12) and (4.13)

$$\begin{aligned} \bar{u}_{2^{s+1}\varrho+n} - \bar{u}_n &= M^{2^{s+1}\varrho}\bar{u}_n - \bar{u}_n \\ &= (M^{2^{s+1}\varrho}-E)\bar{u}_n \\ &= (M^{2^s\varrho}+E)(M^{2^s\varrho}-E)\bar{u}_n \\ &= (M^{2^s\varrho}+E)(2^s\cdot\bar{1}+2^{s+1}\bar{y}_n) \\ &= M^{2^s\varrho}2^s\cdot\bar{1}+2^s\cdot\bar{1}+M^{2^s\varrho}2^{s+1}\bar{y}_n+2^{s+1}\bar{y}_n \\ &\equiv 2\cdot 2^s\cdot\bar{1}+2\cdot 2^{s+1}\bar{y}_n \\ &\equiv 2^{s+1}\cdot\bar{1} \mod 2^{s+2}\ , \end{aligned}$$

with some $\bar{y}_n \in \mathbb{Z}^{k+2}$, which proves (4.11).

(viii) By Lemma 4.19, u_n is uniformly distributed modulo 2 with period length 2ϱ.

Suppose that u_n is uniformly distributed modulo 2^s with period length $2^s\varrho$. This yields, that

$$\#\{n \mid u_n \equiv i \mod 2^s\ ,\ 0 \le n < 2^s\varrho\} = \varrho \qquad \text{for all } 0 \le i < 2^s\ . \tag{4.14}$$

Obviously

$$\begin{aligned}\#\{n \mid u_n \equiv i \mod 2^s,\ 0 \le n < 2^s\varrho\} = \\ \#\{n \mid u_n \equiv i \mod 2^{s+1},\ 0 \le n < 2^s\varrho\} + \\ \#\{n \mid u_n \equiv i + 2^s \mod 2^{s+1},\ 0 \le n < 2^s\varrho\}\end{aligned} \tag{4.15}$$

for all $0 \le i < 2^s$. Furthermore, by (4.11)

$$\begin{aligned}\#\{n \mid u_n \equiv i \mod 2^{s+1},\ 0 \le n < 2^s\varrho\} = \\ \#\{n \mid u_n \equiv i + 2^s \mod 2^{s+1},\ 2^s\varrho \le n < 2^{s+1}\varrho\}\end{aligned}$$

and symmetrically

$$\begin{aligned}\#\{n \mid u_n \equiv i + 2^s \mod 2^{s+1},\ 0 \le n < 2^s\varrho\} = \\ \#\{n \mid u_n \equiv i \mod 2^{s+1},\ 2^s\varrho \le n < 2^{s+1}\varrho\}\end{aligned}$$

for all $0 \le i < 2^2\varrho$.

Hence, using (4.15)

$$\begin{aligned}\#\{n \mid u_n \equiv i \mod 2^{s+1},\ 0 \le n <2^{s+1}\varrho\} = \\ \#\{n \mid u_n \equiv i \mod 2^{s+1},\ 0 \le n < 2^s\varrho\} + \\ \#\{n \mid u_n \equiv i \mod 2^{s+1},\ 2^s\varrho \le n < 2^{s+1}\varrho\} = \\ \#\{n \mid u_n \equiv i + 2^s \mod 2^{s+1},\ 2^s\varrho \le n < 2^{s+1}\varrho\} + \\ \#\{n \mid u_n \equiv i + 2^s \mod 2^{s+1},\ 0 \le n < 2^s\varrho\} = \\ \#\{n \mid u_n \equiv i + 2^s \mod 2^{s+1},\ 0 \le n < 2^{s+1}\varrho\}\end{aligned}$$

for all $0 \le i < 2^s\varrho$.

But,

$$\begin{aligned}\#\{n \mid u_n \equiv i \mod 2^{s+1},\ 0 \le n < 2^{s+1}\varrho\} + \\ \#\{n \mid u_n \equiv i + 2^s \mod 2^{s+1},\ 0 \le n < 2^{s+1}\varrho\} = \\ \#\{n \mid u_n \equiv i \mod 2^s,\ 0 \le n < 2^{s+1}\varrho\} = \\ 2 \cdot \#\{n \mid u_n \equiv i \mod 2^{s+1},\ 0 \le n < 2^s\varrho\} = 2 \cdot \varrho\end{aligned}$$

for all $0 \le i < 2^s\varrho$, whence

$$\#\{n \mid u_n \equiv i \mod 2^{s+1},\ 0 \le n < 2^{s+1}\varrho\} = \varrho$$

for all $0 \le i < 2^{s+1}\varrho$.

Since

$$u_{2^s\varrho} \not\equiv u_n \mod 2^{s+1},$$

thus $2^s\varrho$ is not a period length of u modulo 2^{s+1}, but then by Lemma 3.21 the minimal period length of u modulo 2^{s+1} is $2 \cdot 2^s\varrho = 2^{s+1}\varrho$. Consequently u is uniformly distributed modulo 2^{s+1}.

Finally this leads to the result, u is uniformly distributed modulo 2^s for all $s = 1, 2, \ldots$ and the period length of u modulo s^s is $2^s\varrho = 2^s\mathrm{ord}(Q)$.

Remark 4.21. *Experience shows that the previous theorem may be changed by replacing the words "at least" to "exactly".*

Construction 4.22. *Now we have everything for the construction of a modulo 2^s uniformly distributed linear recurring sequence with large period length.*

1. Choose a suitable integer k and find a polynomial $Q(x)$ which is irreducible modulo 2 and $\deg(Q(x)) = k$. It is better if approximately half of the coefficients are not divisible by 2.

2. Calculate the monic polynomials $P(x) = p_{k+2}x^{k+2} + p_{k+1}x^{k+1} + \cdots + p_0$ and $P'(x)$ such that

$$P(x) \equiv (x^2 - 1)Q(x) \mod 2$$

and $p_0, \ldots, p_{k+1} \in \{0, -1\}$ and

$$P'(x) \equiv (x - 1)Q(x) \mod 2$$

with similar condition on its coefficients. Determine $P_1(x) = P(x)$, $P_2(x) = P_1(x) - 2$, $P_3(x) = P_1(x) - 2x$ and $P_4(x) = P_1(x) - 2x - 2$.

3. Calculate the companion matrices $M_{(i)}$ corresponding to the characteristic polynomials $P_i(x)$. Check $M_{(i)}\bar{1} \equiv \bar{1} \mod 4$. Keep the two matrices which satisfy the congruence and denote them by M_1 and M_2.

4. Compute $\varrho = \mathrm{ord}(Q)$ modulo 2 and $M_1^{2\varrho}$ modulo 4. If $M_1^{2\varrho} \not\equiv E \mod 4$ then $M = M_1$ else $M = M_2$.

5. Choose initial values of the sequence. This can be done by the following: choose random $u_0, u_1, \ldots, u_k$. Set these values as initial values of the linear recurring sequence with characteristic polynomial $P'(x)$. Compute the next element of the sequence u'_{k+1}. Find a random number u_{k+1} satisfying $u_{k+1} \not\equiv u'_{k+1} \mod 2$. The set $u_0, u_1, \ldots, u_k, u_{k+1}$ are suitable initial values for the sequence.

Remark 4.23. *If k is such that $2^k - 1$ is a – so called Mersenne – prime, then by Proposition 4.7, ord$(Q) = 2^k - 1$, i.e. maximal as a function of k.*

If we choose P such that its coefficient are 0 and -1, except the leading coefficient which is 1, then the computation of the elements of the recurring sequence is very fast, since there are no need for multiplication, only addition. Further, because of the inner representation of the numbers in computers, also the reduction modulo 2^s can be easily performed. (By a simple logical bit operation.)

Since we can obtain not only 1 digit, but arbitrary length random numbers, thus we have a very effective method for construct large pseudo-primes. (In the opposite case if we would need large numbers, we have to compose from bits, but then it is more difficult to prove uniform distribution.)

In Appendix B we give an example for a high order linear recurring sequence.

Example 4.24. *In a small example we demonstrate the use of Construction 4.22. In particular, we will follow the consideration of Remark 4.23.*

1. Let $k = 3$ and choose a random polynomial of degree 3, which is irreducible modulo 2, say $Q(x) = x^3 + x^2 + 1$.

2. We put

$$P(x) = x^5 - x^4 - x^3 - 1 \equiv (x^3 + x^2 + 1)(x^2 - 1) \mod 2$$

and

$$P'(x) = x^4 - x^2 - x - 1 \equiv (x^3 + x^2 + 1)(x - 1) \mod 2 .$$

Thus we have

$$\begin{aligned} P_1(x) &= x^5 - x^4 - x^3 - 1 \\ P_2(x) &= x^5 - x^4 - x^3 - 3 \\ P_3(x) &= x^5 - x^4 - x^3 - 2x - 1 \\ P_4(x) &= x^5 - x^4 - x^3 - 2x - 3 . \end{aligned}$$

3. Following the steps of the construction, we compute the companion matrices, corresponding to the proper recurrence relations:

$$M_{(1)} = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix} \qquad M_{(2)} = \begin{pmatrix} 1 & 1 & 0 & 0 & 3 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

$$M_{(3)} = \begin{pmatrix} 1 & 1 & 0 & 2 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix} \qquad M_{(4)} = \begin{pmatrix} 1 & 1 & 0 & 2 & 3 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix} .$$

Computing $M_{(1)}\bar{1}$, we obtain

$$M_{(1)}\bar{1} = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 3 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} \not\equiv \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} \mod 4 .$$

By **(iii)** of the proof of Theorem 4.20, we can set $M_1 = M_{(2)}$ and $M_2 = M_{(3)}$.

4. By Remark 4.23, $\varrho = 2^3 - 1 = 7$. We can use fast exponentiation for the calculation of M_1^{14} and we get

$$M_1^{14} \equiv \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \mod 4 ,$$

whence

$$M = M_2 = M_{(3)} = \begin{pmatrix} 1 & 1 & 0 & 2 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix} .$$

5. Suppose, that we want to construct a sequence of bytes. Then $s = 8$. We can choose random values for the first 4 elements, say

$$u_0 = 113 , \quad u_1 = 5 , \quad u_2 = 209 \quad \text{and} \quad u_3 = 198 .$$

Satisfying the recurrence relation defined by $P'(x)$, the next value of the sequence is $u'_4 = 113 + 5 + 209 \equiv 1 \mod 2$. Hence u_4 can be any number divisible by 2, say 66.

Thus we have constructed a linear recurring sequence, with recurrence relation

$$u_{n+5} = u_{n+4} + u_{n+3} + 2u_{n+1} + u_n$$

and initial values

$$u_0 = 113 , \quad u_1 = 5 , \quad u_2 = 209 \quad , u_3 = 198 \quad \text{and} \quad u_4 = 66 .$$

Reducing the sequence modulo 256, by Theorem 4.20, we obtain a pseudo random byte sequence, which has period length $7 \cdot 256 = 1792$.

The first few values of the sequence:

113 , 5 , 209 , 198 , 66 , 131 , 108 , 76 , 2 , 150 , 243 , 141 , 208 , 139 , 215 , 111 .

Chapter 5

Sequences with non-uniform distribution

In the previous chapters we gave the background to construct uniformly distributed linear recurring sequences. However in practice, it is very often required to have a random sequence with a specific non uniform distribution. There are several way to do this. Well known for instance, that if we know the inverse of the distribution function F of the required distribution, then simply use a uniformly distributed sequence u with the transformation $F^{-1}(u)$ to have the required property. In this chapter we will provide another method to construct non-uniformly distributed pseudo-random sequences from uniformly distributed sequences. In particular, we will generate sequences with Gaussian distribution. To reach our goal, we use the central limit distribution theorem. Furthermore, we determine the "goodness" of the obtained Gaussian sequence, calculating its discrepancy. Finally, our method is suitable also for testing randomness of sequences. We should mention here, that the results of this chapter are contained in [20].

Definitions 5.1. *Let $(X, \mathfrak{F}, \mu)$ be a probability space, let $\mathfrak{U} \subseteq \mathfrak{F}$ be a family of measurable sets of X and let ξ be a sequence in X.*

Then we say that ξ is μ **distributed with respect to** *$\mathfrak{U}$ if*

$$\lim_{N\to\infty} \frac{A(N,B,\xi)}{N} = \mu(B) \quad \textit{for all} \quad B \in \mathfrak{U}\ , \tag{5.1}$$

where

$$A(N,B,\xi) = \#\{\xi_n | n < N, \xi_n \in B\}\ .$$

The **discrepancy** *of ξ with respect to μ and $\mathfrak{U}$ is defined by*

$$D_N(\xi,\mu,\mathfrak{U}) = \sup_{B\in\mathfrak{U}} \left| \frac{A(N,B,\xi)}{N} - \mu(B) \right|. \tag{5.2}$$

The family of measurable sets, $\mathfrak{U}$ is called a **discrepancy system** *(cf. [10]). Important cases for $\mathfrak{U}$ in the Euclidean space are for instance the axis-parallel intervals or the family of all balls or of all convex sets etc.*

Define the following vector sequence:

$$\bar{\xi}_n^{(k)} = (\xi_n, \ldots, \xi_{n+k-1}) \quad \textit{for all} \quad n \in \mathbb{N}\ .$$

A sequence ξ in X is called **completely μ-distributed** *(for short: μ-c.d.), if $\bar{\xi}^{(k)}$ is $\mu^{(k)}$-distributed in X^k with respect to $\mathfrak{U}^k$ for every $k \in \mathbb{N}$ where $\mu^{(k)}$ is the k-fold product measure of μ and $\mathfrak{U}^k$ is – as usual – the cartesian product of $\mathfrak{U}$.*

If $X \subseteq \mathbb{C}$ then ξ is called **pseudo-random number sequence**.

Let $X \subset \mathbb{R}$ be a bounded interval, $\mathfrak{F} = \mathfrak{B}$ be the Borel measurable sets of X, $\mu = \lambda$ be the normalized Lebesgue measure (i.e. $\lambda(X) = 1$) and let $\mathfrak{I}$ be the family of all intervals of $\mathfrak{B}$. If ξ is λ distributed with respect to $\mathfrak{I}$, then we will call it **uniformly distributed** *(for short u.d.). We should remark, that this sense of uniform distribution is the generalization of Definition 1.12.*

If ξ is λ-c.d. we will call it **completely uniformly distributed** *and abbreviate it by c.u.d.*

Note that completely uniform distribution is suitable for expressing "strong" randomness.

In the followings, let ξ be a u.d. sequence in the interval $\left[-\frac{1}{2}, \frac{1}{2}\right]$ and let

$$F_k : \left[-\frac{1}{2}, \frac{1}{2}\right]^k \to \mathbb{R} \tag{5.3}$$

be a measurable mapping with $k \in \mathbb{N}$.

Consider the induced measure μ of the k-dimensional Lebesgue measure $\lambda^{(k)}$ on $\left[-\frac{1}{2}, \frac{1}{2}\right]^k$ by

$$\mu(B) = \lambda^{(k)}(F_k^{-1}(B)) \qquad (B \in \mathfrak{B}). \tag{5.4}$$

Furthermore, we set

$$\eta_n = F_k(\bar{\xi}_n^{(k)}) \ . \tag{5.5}$$

Lemma 5.2. *Let ξ be a sequence in $\mathbb{R}^k$, $\mathfrak{I}$ be the family of all axis-parallel intervals and let $\mathfrak{C}$ be the family of all convex sets in $\mathbb{R}^k$ and let $N \in \mathbb{N}$. Then*

$$D_N(\xi, \lambda, \mathfrak{I}) \le D_N(\xi, \lambda, \mathfrak{C}) \le (4k^{3/2} + 1) D_N(\xi, \lambda, \mathfrak{I})^{1/k}$$

Proof. See e.g. Theorem 1.6 in [23]. □

Lemma 5.3. *Let F_k be a measurable function satisfying* (5.3) *with the property that*

$$F_k^{-1}(I) \quad \text{is convex for all interval} \quad I \subseteq \mathbb{R} \tag{5.6}$$

and let ξ be c.u.d. Then η – given by (5.5) *– is μ-c.d., where μ is the derived measure defined by* (5.4). *Furthermore, the discrepancy estimate* (5.7) *can be established.*

Proof. Define

$$F_{k,m}(x_1, \ldots, x_{k+m-1}) = \left(F_k(x_1, \ldots, x_k), F_k(x_2, \ldots, x_{k+1}), \ldots, F_k(x_m, \ldots, x_{m+k-1})\right)$$

and let $\mathfrak{I}^{(m)}$ be the family of all axis-parallel intervals in $\mathbb{R}^m$ and $\mathfrak{C}^{(k+m-1)}$ be the family of all convex sets in $\mathbb{R}^{k+m-1}$ for arbitrary $m \in \mathbb{N}$.

Note that $F_{k,m} : \left[-\frac{1}{2}, \frac{1}{2}\right]^{k+m-1} \to \mathbb{R}^m$ is measurable.

Because of (5.6), if B is an axis-parallel interval in $\mathbb{R}^m$, then ${F_{k,m}}^{-1}(B)$ is a convex sets in $\left[-\frac{1}{2}, \frac{1}{2}\right]^{k+m-1}$. Thus, we get

$$\begin{aligned}
&D_n\left(\bar{\eta}^{(m)}, \mu^{(m)}, \mathfrak{J}^{(m)}\right) \\
&\quad = \sup_{B \in \mathfrak{J}^{(m)}} \left| \frac{A(n, B, \bar{\eta}^{(m)})}{n} - \mu^{(m)}(B) \right| \\
&\quad \le \sup_{B \in \mathfrak{J}^{(m)}} \left| \frac{A\left(n, {F_{k,m}}^{-1}(B), \bar{\xi}^{(k+m-1)}\right)}{n} - \lambda^{(k+m-1)}\left({F_{k,m}}^{-1}(B)\right) \right| \\
&\quad \le \sup_{C \in \mathfrak{C}^{(k+m-1)}} \left| \frac{A\left(n, C, \bar{\xi}^{(k+m-1)}\right)}{n} - \lambda^{(k+m-1)}(C) \right| \\
&\quad = D_n\left(\bar{\xi}^{(k+m-1)}, \lambda^{(k+m-1)}, \mathfrak{C}^{(k+m-1)}\right) \ ,
\end{aligned}$$

whence by Lemma 5.2, we get

$$\begin{aligned}
&D_n\left(\bar{\eta}^{(m)}, \mu^{(m)}, \mathfrak{J}^{(m)}\right) \\
&\le \left(4(k+m-1)^{3/2}+1\right)\left(D_n\left(\bar{\xi}^{(k+m-1)}, \lambda^{(k+m-1)}, \mathfrak{J}^{(k+m-1)}\right)\right)^{\frac{1}{k+m-1}} \ .
\end{aligned} \tag{5.7}$$

Since ξ is c.u.d. we get $D_n\left(\bar{\eta}^{(m)}, \mu^{(m)}, \mathfrak{U}^{(m)}\right) \to 0$ as $n \to \infty$. $\square$

Remark 5.4. *Using the general inequality of Niederreiter and Wills* [33]*, we obtain a somewhat better result*

$$\begin{aligned}
&D_n\left(\bar{\eta}^{(m)}, \mu^{(m)}, \mathfrak{J}^{(m)}\right) \\
&\le (4(k+m-1)+1)\left(D_n\left(\bar{\xi}^{(k+m-1)}, \lambda^{(k+m-1)}, \mathfrak{J}^{(k+m-1)}\right)\right)^{\frac{1}{k+m-1}} \ .
\end{aligned} \tag{5.8}$$

For various applications of transformations of random numbers we refer to [8].

To construct pseudo-random number sequences with different distributions we just have to find a transformation which converts the Lebesgue measure into the required probability measure by $\mu(B) = \lambda^{(k)}\left(F_k^{-1}(B)\right)$ and if ξ is a c.u.d. sequence, then the sequence $\eta = F_k(\bar{\xi}^{(k)})$ will have the desired distribution.

The main problem is that finding such an F_k is usually not evident. As we will see, for practical applications it is sufficient to find approximations of the required distribution. For example, if we would like to have a pseudo-random number sequence close to Gaussian distribution, then using the Central Limit Theorem or one of its quantified versions, the Berry-Esséen Theorem, we can prove that there is a possibility to get the expected sequence.

Theorem 5.5 (Berry-Esséen Theorem). *Let $k \geq 1$ be an integer, $\xi_1, \ldots, \xi_k$ be independent random variables in $\mathbb{R}$, each with zero mean, let σ_i^2 be the variance and ϱ_i be the absolute third moment of ξ_i for $1 \leq i \leq k$ and let*

$$\sigma^2 = \frac{1}{k}\sum_{i=1}^{k}\sigma_i^2 \qquad \text{and} \qquad \varrho = \frac{1}{k}\sum_{i=1}^{k}\varrho_i$$

be the average variance and the average absolute third moment of $\xi_1, \ldots, \xi_k$, respectively. Define the random variable

$$\eta = \frac{1}{\sqrt{k}\sigma}\sum_{i=1}^{k}\xi_i \ .$$

Let μ be the probability measure corresponding to η and let γ be the probability measure corresponding to the standard Gaussian distribution.

If none of $\varrho_1, \ldots, \varrho_k, \sigma$ is vanishing, then

$$\sup_{B\in\mathfrak{L}} |\mu(B) - \gamma(B)| \leq \frac{11}{4\sqrt{k}}\frac{\varrho}{\sigma^3} \ ,$$

where $\mathfrak{L}$ is the family of all intervals $]-\infty, x[$.

Proof. See e.g. Theorem 12.4 in [1] $\square$

Lemma 5.6. *Let ξ be a c.u.d. sequence in $\left[-\frac{1}{2}, \frac{1}{2}\right]$, let k be a positive integer, let $0 < \varepsilon \leq 1$ and let*

$$F_k : \mathbb{R}^k \to \mathbb{R}$$

be a linear transformation, such that

$$F_k(\bar{x}) = \sum_{i=1}^{k} f_i x_i \ ,$$

where $\bar{x} = (x_1, \ldots, x_k)$ and $f_1, \ldots, f_k \in \mathbb{R}$, such that

$$|f_i| \geq \varepsilon\frac{2\sqrt{3}}{\sqrt{k}} \quad \text{for all} \quad 1 \leq i \leq k \ . \tag{5.9}$$

If

$$\sum_{i=1}^{k} f_i^2 = 12 \ ,$$

then the sequence η, defined by

$$\eta_m = F_k\left(\bar{\xi}_m^{(k)}\right) \quad \text{for all} \quad m \in \mathbb{N} \ ,$$

has discrepancy

$$D_n(\eta, \gamma, \mathfrak{I}) \leq \left(4k^{\frac{3}{2}} + 1\right) D_n\left(\bar{\xi}^{(k)}, \lambda^{(k)}, \mathfrak{I}^{(k)}\right)^{\frac{1}{k}} + \frac{33\sqrt{3}}{8}\sqrt{(1-\varepsilon^2) + \frac{\varepsilon^2}{k}} \ ,$$

where $\mathfrak{I}$ and $\mathfrak{I}^{(k)}$ are the families of all the intervals and axis-parallel intervals in $\mathbb{R}$ and in $\mathbb{R}^k$, respectively, γ is the probability measure corresponding to the standardized Gaussian distribution and $\lambda^{(k)}$ is the Lebesgue measure in $\mathbb{R}^k$.

Proof. By the definition of $D_n(\eta, \gamma, \mathfrak{I})$ and using Lemma 5.3, we have

$$
\begin{aligned}
D_n(\eta,\gamma,\mathfrak{I}) &= \sup_{B\in\mathfrak{I}} \left| \frac{A(n,B,\eta)}{n} - \gamma(B) \right| \\
&\le \sup_{B\in\mathfrak{I}} \left(\left| \frac{A(n,B,\eta)}{n} - \mu(B) \right| + |\mu(B)-\gamma(B)| \right) \\
&\le \sup_{B\in\mathfrak{I}} \left| \frac{A(n,B,\eta)}{n} - \mu(B) \right| + \sup_{B\in\mathfrak{I}} |\mu(B)-\gamma(B)| \\
&\le \left(4k^{\frac{3}{2}}+1\right) D_n\left(\bar{\xi}^{(k)}, \lambda^{(k)}, \mathfrak{I}^{(k)}\right)^{\frac{1}{k}} + \sup_{B\in\mathfrak{I}} |\mu(B)-\gamma(B)| \ ,
\end{aligned}
\tag{5.10}
$$

where μ is the measure corresponding to the distribution of η.

Since the sequence ξ has variance $\frac{1}{12}$, the average variance σ^2 of the random variables

$$f_1\xi_m, f_2\xi_{m+1}, \dots, f_k\xi_{m+k-1}$$

is

$$\sigma^2 = \frac{1}{k}\sum_{i=1}^{k}\left(f_i^2\frac{1}{12}\right) = \frac{1}{k}\frac{1}{12}\sum_{i=1}^{k} f_i^2 = \frac{1}{k}\left(\frac{1}{12}\right)\cdot 12 = \frac{1}{k} \ ,$$

whence $\sqrt{k}\sigma = 1$ and thus

$$\eta_m = F_k\left(\bar{\xi}_m^{(k)}\right) = \frac{1}{\sqrt{k}\sigma}\sum_{i=1}^{k} f_i\xi_{m+i-1} \ . \tag{5.11}$$

Furthermore, by (5.9),

$$f_i^2 > \varepsilon^2\frac{12}{k} \quad \text{for every} \quad 1 \le i \le k \ .$$

If $1 \le j \le k$ is such that

$$|f_j| = \max_{1\le i\le k} |f_i| \ ,$$

then

$$12 = \sum_{i=1}^{k} f_i^2 > f_j^2 + (k-1)\varepsilon^2\frac{12}{k} \ ,$$

whence

$$\max_{1\le i\le k} |f_i| < \sqrt{12-(k-1)\varepsilon^2\frac{12}{k}} = 2\sqrt{3}\sqrt{(1-\varepsilon^2)+\frac{\varepsilon^2}{k}} \ . \tag{5.12}$$

Let $B \in \mathfrak{I}$, such that $\inf B = x$ and $\sup B = y$. Then

$$\begin{aligned}|\mu(B) - \gamma(B)| &= |\mu(\,]-\infty, y[\,) - \mu(\,]-\infty, x[\,) - \gamma(\,]-\infty, y[\,) + \gamma(\,]-\infty, x[\,)| \\ &\le |\mu(\,]-\infty, y[\,) - \gamma(\,]-\infty, y[\,)| + |\mu(\,]-\infty, x[\,) - \gamma(\,]-\infty, x[\,)| \ .\end{aligned}$$

Hence, by (5.11), (5.12) and Theorem 5.5, noticing that the third absolute moment of ξ is equal to $\frac{1}{32}$, we obtain

$$\begin{aligned}\sup_{B\in\mathfrak{I}} |\mu(B) - \gamma(B)| &\le 2 \sup_{B'\in\mathfrak{L}} |\mu(B') - \gamma(B')| \\ &\le 2\frac{11}{4\sqrt{k}} \left(\frac{1}{\sqrt{k}}\right)^{-3} \left(\frac{1}{k}\sum_{i=1}^{k} \left(|f_i|^3 \frac{1}{32}\right)\right) \\ &= \frac{11}{64}\sum_{i=1}^{k} |f_i|^3 \\ &\le \frac{11}{64} \max_{1\le i\le k} |f_i| \sum_{i=1}^{k} |f_i|^2 \\ &\le \frac{11}{64} 2\sqrt{3}\sqrt{(1-\varepsilon^2) + \frac{\varepsilon^2}{k}} \cdot 12 \\ &= \frac{33\sqrt{3}}{8}\sqrt{(1-\varepsilon^2) + \frac{\varepsilon^2}{k}} \ .\end{aligned}$$

Here, as before, $\mathfrak{L}$ is the family of all intervals $]-\infty, x[$.

Hence, by (5.10) the lemma follows. □

Corollary 5.7. *With the conditions of Lemma 5.6, if F_k is such that the corresponding*

$$|f_1| = \cdots = |f_k| = \frac{2\sqrt{3}}{\sqrt{k}} \ ,$$

then

$$D_n(\eta, \gamma, \mathfrak{I}) \le \left(4k^{\frac{3}{2}} + 1\right) D_n\left(\bar{\xi}^{(k)}, \lambda^{(k)}, \mathfrak{I}^{(k)}\right)^{\frac{1}{k}} + \frac{33\sqrt{3}}{8\sqrt{k}} \ ,$$

Proof. Substituting ε by 1, we obtain that

$$\frac{33\sqrt{3}}{8}\sqrt{(1-\varepsilon^2) + \frac{\varepsilon^2}{k}} = \frac{33\sqrt{3}}{8}\sqrt{\frac{1}{k}} = \frac{33\sqrt{3}}{8\sqrt{k}} \ ,$$

whence by Lemma 5.6, we obtain the statement. □

Remark 5.8. *We can choose ξ to be a very special c.u.d. sequence with a strong property, namely, that there exists an increasing sequence of k_n $(n = 0, 1, \dots)$, such that*

$$D_n\left(\bar{\xi}^{(k_n)}, \lambda^{(k_n)}, \mathfrak{I}^{(k_n)}\right) \to 0 \quad as \quad n \to \infty \ ,$$

where $\lambda^{(k_n)}$ is the k_n dimensional Lebesgue-measure and $\mathfrak{I}^{(k_n)}$ is the family of axis-parallel intervals in $\mathbb{R}^{k_n}$.

These kinds of sequences (in more general settings) are studied in [12] and [17]. In [12] the following result is proved:

Theorem 5.9. *Let $0 < \Theta < \frac{1}{2}$ be fixed, k_n be a sequence of positive integers with*

$$k_n \leq (\log n)^{\Theta}$$

if $n \in \mathbb{N}$ is sufficiently large, let p_n be a sequence of distinct positive integers and let ε be an arbitrary positive real number.

Then for almost all real $s \times s$ matrix M with dominating eigenvalue bigger than 1 there exists a constant c depending on M, ε, and the given integral sequences p and k, such that

$$D_n(\bar{\xi}^{(k_n)}, \lambda^{(s^2 k_n)}, \mathfrak{I}^{(s^2 k_n)}) \leq c n^{-\frac{1}{2}+\varepsilon} \quad \textit{for all} \quad n \in \mathbb{N} \ ,$$

where

$$\xi_m = M^{p_m} \mod 1 \ ,$$

furthermore, $\lambda^{(s^2 k_n)}$ and $\mathfrak{I}^{(s^2 k_n)}$ are as given above.

Remark 5.10. *The metric result of* [12] *can be extended to general exponent sequences as it is done in* [17] *for the case $s = 1$.*

Lemma 5.11. *Let $0 < \Theta < 1$ be fixed, k_n be an increasing sequence with $\lim k_n = \infty$, such that*

$$k_n \leq (\log n)^{\Theta} \ , \tag{5.13}$$

let ξ be a sequence of numbers in the interval $\left[-\frac{1}{2}, \frac{1}{2}\right]$, such that

$$D_n(\bar{\xi}^{(k_n)}, \lambda^{(k_n)}, \mathfrak{I}^{(k_n)}) \leq c \cdot n^{-\frac{1}{2}+\varepsilon} \tag{5.14}$$

with $c > 0$ and $0 < \varepsilon < \frac{1}{2}$ and let

$$F_n : \mathbb{R}^{k_n} \to \mathbb{R}$$

be an arbitrary sequence of linear functionals, satisfying

$$F_n(\bar{x}) = \sum_{i=1}^{k_n} f_{n,i} x_i \qquad \textit{with} \qquad |f_{n,i}| = \frac{2\sqrt{3}}{\sqrt{k_n}} \quad \forall i \in \{1, \ldots k_n\} \ .$$

Then the sequence

$$\eta_n := F_n\left(\bar{\xi}_n^{(k_n)}\right)$$

is a completely Gaussian distributed sequence.

Proof. If n is big enough, then $c \cdot n^{-1/2+\varepsilon} < 1$. Hence, by (5.13), (5.14) and by Corollary 5.7, we have

$$\begin{aligned} D_n(\eta,\gamma,\mathfrak{I}) &= \left(4\,(k_n)^{\frac{3}{2}}+1\right) D_n\left(\bar{\xi}^{(k_n)},\lambda^{(k_n)},\mathfrak{I}^{(k_n)}\right)^{1/k_n} + \frac{33\sqrt{3}}{8\sqrt{k_n}} \\ &\le \left(4\left(\log(n)^{\Theta}\right)^{\frac{3}{2}}+1\right)\left(c\cdot n^{-\frac{1}{2}+\varepsilon}\right)^{1/\log(n)^{\Theta}} + \frac{33\sqrt{3}}{8\sqrt{k_n}} \\ &\le 5\left(\log(n)^{\Theta}\right)^{\frac{3}{2}}\left(c\cdot n^{-\frac{1}{2}+\varepsilon}\right)^{1/\log(n)^{\Theta}} + \frac{33\sqrt{3}}{8\sqrt{k_n}} \\ &= 5\log(n)^{\frac{3}{2}\Theta} c^{1/\log(n)^{\Theta}} \cdot e^{(\varepsilon-1/2)\log(n)/\log(n)^{\Theta}} + \frac{33\sqrt{3}}{8\sqrt{k_n}} \\ &= 5\log(n)^{\frac{3}{2}\Theta} c^{1/\log(n)^{\Theta}} \cdot e^{(\varepsilon-1/2)\log(n)^{1-\Theta}} + \frac{33\sqrt{3}}{8\sqrt{k_n}} \\ &= 5\log(n)^{\frac{3}{2}\Theta} c^{1/\log(n)^{\Theta}} \cdot n^{(\varepsilon-1/2)(1-\Theta)} + \frac{33\sqrt{3}}{8\sqrt{k_n}}\ . \end{aligned}$$

Clearly,

$$-\frac{1}{2} < (\varepsilon-1/2)(1-\Theta) < 0\ ,$$

whence

$$\log(n)^{\frac{3}{2}\Theta} n^{(\varepsilon-1/2)(1-\Theta)} \to 0\ .$$

Furthermore,

$$c^{1/\log(n)^{\Theta}} \to 1 \qquad \text{and} \qquad \frac{33\sqrt{3}}{8\sqrt{k_n}} \to 0\ ,$$

consequently,

$$D_n(\eta,\gamma,\mathfrak{I}) \to 0\ . \quad \square$$

Remark 5.12. *One should be very careful with the conditions stated in the results. In the followings we give an example of a u.d., but not c.u.d. sequence, such that its linear transformation is not Gaussian distributed.*

Example. Let

$$k_n = \max\left\{ j \mid \sum_{m=1}^{j} m \le n \right\}\ ,$$

let

$$\kappa(n) = \sum_{m=1}^{k_n} m \quad \text{for all} \quad n \in \mathbb{N}$$

and let ξ_n be the sequence defined by

$$\xi_n = \frac{n-\kappa(n)}{k_n} - \frac{1}{2}\quad .$$

Further, we set

$$\eta_n = \frac{2\sqrt{3}}{\sqrt{k_n}} \sum_{j=0}^{k_n} (-1)^j \xi_{n+j} \ .$$

We claim that ξ is u.d. in $\left[-\frac{1}{2}, \frac{1}{2}\right]$, but η is not Gaussian distributed. Clearly,

$$\kappa(n) = \frac{k_n^2 + k_n}{2} \tag{5.15}$$

and

$$\kappa(n) \le n \le \kappa(n) + k_n \ ,$$

whence

$$0 \le n - \kappa(n) \le k_n \tag{5.16}$$

and thus

$$\xi_n \in \left[-\frac{1}{2}, \frac{1}{2}\right] \quad \text{for all} \quad n \in \mathbb{N} \ .$$

Let

$$-\frac{1}{2} \le a < b \le \frac{1}{2}$$

and let

$$\widehat{A}(n_1, n_2, [a,b], \xi) = \#\left\{j \mid n_2 \le j < n_1 \ , \ \xi_j \in [a,b]\right\} \ .$$

Then $\lambda([a,b]) = b - a$ and

$$\begin{aligned} A(n, [a,b], \xi) &= \widehat{A}(n, \kappa(n), [a,b], \xi) + A(\kappa(n), [a,b], \xi) \\ &= \widehat{A}(n, \kappa(n), [a,b], \xi) + \sum_{m=2}^{k_n} \widehat{A}\left(\sum_{j=1}^{m} j, \sum_{j=1}^{m-1} j, [a,b], \xi\right) + A(1, [a,b], \xi) \ . \end{aligned}$$

Since

$$0 \le \widehat{A}(n, \kappa(n), [a,b], \xi) \le k_n \ ,$$

$$m(b-a) - 1 \le \widehat{A}\left(\sum_{j=1}^{m} j, \sum_{j=1}^{m-1} j, [a,b], \xi\right) \le m(b-a) + 1$$

and

$$0 \le A(1, [a,b], \xi) \le 1 \ ,$$

thus

$$\sum_{m=2}^{k_n} (m(b-a) - 1) \le A(n, [a,b], \xi) \le k_n + \sum_{m=2}^{k_n} (m(b-a) + 1) + 1 \ ,$$

i.e.

$$(b-a)\sum_{m=2}^{k_n} m - k_n + 1 \le A(n,[a,b],\xi) \le k_n + (b-a)\sum_{m=2}^{k_n} m + k_n - 1 + 1 \ ,$$

which is equivalent to

$$(b-a)(\kappa(n)-1) - k_n + 1 \le A(n,[a,b],\xi) \le 2k_n + (b-a)(\kappa(n)-1) \ .$$

Hence by (5.15) and (5.16),

$$\begin{aligned}
(b-a) - \frac{2}{k_n+1} &< (b-a) - \frac{k_n-1}{\kappa(n)} \\
&< \frac{(b-a)(\kappa(n)-1) - k_n + 1}{\kappa(n)} \\
&\le \frac{(b-a)(\kappa(n)-1) - k_n + 1}{n} \\
&\le \frac{A(n,[a,b],\xi)}{n} \\
&\le \frac{2k_n + (b-a)(\kappa(n)-1)}{n} \\
&\le \frac{2k_n + (b-a)(\kappa(n)-1)}{\kappa(n)} \\
&< (b-a) + \frac{2k_n}{\kappa(n)} \\
&= (b-a) + \frac{4}{k_n+1} \ .
\end{aligned}$$

This yields that

$$\lim_{n\to\infty} \frac{A(n,[a,b],\xi)}{n} = b-a \ ,$$

i.e. by definition, ξ is uniformly distributed.

Observe now the sequence η. Fix $n \in \mathbb{N}$ and let $0 \le l \le k_n$, such that

$$n + l = \kappa(n) + k_n \ .$$

Then

$$\begin{aligned}
\eta_n &= \frac{2\sqrt{3}}{\sqrt{k_n}} \sum_{j=0}^{k_n} (-1)^j \xi_{n+j} = \\
&= \frac{2\sqrt{3}}{\sqrt{k_n}} \left(\sum_{j=0}^{l} (-1)^j \xi_{n+j} + \sum_{j=l+1}^{k_n} (-1)^j \xi_{n+j} \right) \ .
\end{aligned} \tag{5.17}$$

We recall that

$$\xi_{n+l+1} = \xi_{\kappa(n)+k_n+1} = -\frac{1}{2}$$

and

$$\xi_{n+l} = \xi_{\kappa(n)+k_n} = \frac{1}{2} \ .$$

If l is odd, then

$$\sum_{j=0}^{l}(-1)^j \xi_{n+j} = -\frac{1}{k_n}\frac{l+1}{2} \ ,$$

if l is even, then

$$\sum_{j=0}^{l}(-1)^j \xi_{n+j} = -\frac{1}{k_n}\frac{l}{2} + \xi_{n+l} = -\frac{1}{k_n}\frac{l}{2} + \frac{1}{2} \ ,$$

whence

$$-\frac{l}{2k_n} - \frac{1}{2k_n} \le \sum_{j=0}^{l}(-1)^j \xi_{n+j} \le -\frac{l}{2k_n} + \frac{1}{2} \ . \tag{5.18}$$

Similarly, if both l and k_n are odd, then

$$\sum_{j=l+1}^{k_n} (-1)^j \xi_{n+j} = \frac{1}{k_n+1}\frac{k_n-l}{2} = \frac{1}{2} - \frac{l+1}{2(k_n+1)} \ ,$$

if l is odd, but k_n is even, then

$$\sum_{j=l+1}^{k_n} (-1)^j \xi_{n+j} = \frac{1}{k_n+1}\frac{k_n-l-1}{2} + \xi_{n+k_n} = \frac{1}{2} - \frac{l+2}{2(k_n+1)} + \xi_{n+k_n} \ ,$$

if l is even, but k_n is odd, then

$$\begin{aligned}\sum_{j=l+1}^{k_n} (-1)^j \xi_{n+j} &= -\xi_{n+l+1} + \frac{1}{k_n+1}\frac{k_n-l-1}{2} \\ &= -\xi_{n+l+1} + \frac{1}{2} - \frac{l+2}{2(k_n+1)} \\ &= \frac{1}{2} + \frac{1}{2} - \frac{l+2}{2(k_n+1)} \\ &= 1 - \frac{l+2}{2(k_n+1)}\end{aligned}$$

and if both l and k_n are even, then

$$\begin{aligned}\sum_{j=l+1}^{k_n} (-1)^j \xi_{n+j} &= -\xi_{n+l+1} + \frac{1}{k_n+1}\frac{k_n-l-2}{2} + \xi_{n+k_n} \\ &= 1 - \frac{l+3}{2(k_n+1)} + \xi_{n+k_n} \ .\end{aligned}$$

Summarizing the four cases and using that

$$-\frac{1}{2} \le \xi_{n+k_n} \le \frac{1}{2} \ ,$$

we obtain

$$-\frac{l+3}{2(k_n+1)} \le \sum_{j=l+1}^{k_n} (-1)^j \xi_{n+j} \le \frac{3}{2} - \frac{l+1}{2(k_n+1)} \ .$$

Hence by (5.17) and (5.18), using that $0 \le l \le k_n$, we have

$$\begin{aligned}
-\frac{4\sqrt{3}}{\sqrt{k_n}} &< \frac{2\sqrt{3}}{\sqrt{k_n}} \left(-\frac{1}{2} - \frac{1}{2k_n} - \frac{1}{2} - \frac{2}{2(k_n+1)} \right) \\
&= \frac{2\sqrt{3}}{\sqrt{k_n}} \left(-\frac{k_n}{2k_n} - \frac{1}{2k_n} - \frac{k_n+3}{2(k_n+1)} \right) \\
&\le \frac{2\sqrt{3}}{\sqrt{k_n}} \left(-\frac{l}{2k_n} - \frac{1}{2k_n} - \frac{l+3}{2(k_n+1)} \right) \\
&\le \eta_n \\
&\le \frac{2\sqrt{3}}{\sqrt{k_n}} \left(-\frac{l}{2k_n} + \frac{1}{2} + \frac{3}{2} - \frac{l+1}{2(k_n+1)} \right) \\
&\le \frac{2\sqrt{3}}{\sqrt{k_n}} \left(2 - \frac{1}{2(k_n+1)} \right) \\
&< \frac{4\sqrt{3}}{\sqrt{k_n}} \ .
\end{aligned}$$

But this yields that η is convergent to zero, i.e. it cannot have Gaussian distribution. □

Remark 5.13. *If we want to use a pseudo-random number sequence in practice, it is required to be a 'good' random sequence. Only the first approximation of goodness is that the sequence has the expected distribution. The 'randomness' is higher, if the sequence passes more statistical tests. (Of course, the different tests have different weights in the classification at a particular use of the pseudo-random sequence.) In Appendix C we make some experimental examinations of several sequences of numbers. Remark 5.12 also gives an idea to test u.d. sequences by transforming them into another distribution and testing the new sequence by the usual tests.*

Chapter 6

Application of linear recurring sequences

Let us consider the trinomial $x^n - Bx^k - A \in \mathbb{Z}[x]$. Ribenboim [38] has shown that if $k = 1$, then for a fixed n and B there exist only finitely many A's for which the trinomial is divisible by a quadratic polynomial and similarly if n and A are fixed, then there exist only finitely many B's for which the trinomial has a quadratic factor. He used only elementary steps in the proof.

Schinzel in [40] presented a much more general result, in which he proved among others that for a fixed A there exist only finitely many n's,k's and B's for which the trinomial is divisible by any polynomial. He could prove a similar result for a fixed B, too. His proof is however not an elementary one.

We are also able to generalize Ribenboim's result by extending his proof but keeping its elementariness. Our result is less general than Schinzel's one. The results of this chapter are basically identical to the results of [21].

During this chapter we will use the notation $\chi(n)$ for the parity function of $n \in \mathbb{N}$, i.e.

$$\chi(n) = \begin{cases} 0 & \text{if} \quad n \equiv 0 \mod 2 \\ 1 & \text{if} \quad n \equiv 1 \mod 2 \end{cases} .$$

Let R be a commutative ring, and let $u_n \in R$ be a second-order linear recurring sequence with recurrence relation

$$u_n = u_{n-1} + a u_{n-2} \quad \text{for} \quad n \geq 2 \ ,$$

with $a \in R$ and initial values $u_1 = u_0 = 1$. Let us define as in Chapter 1 the state vector

$$\bar{u}_n = \begin{pmatrix} u_{n+1} \\ u_n \end{pmatrix}$$

and let M be the companion matrix of the sequence, i.e.

$$M = \begin{pmatrix} 1 & a \\ 1 & 0 \end{pmatrix} \ .$$

With these definitions we have $\bar{u}_{n+1} = M\bar{u}_n$. We remark that the sequence can be extended with the value $u_{-1} = 0$.

Lemma 6.1. *Let $0 \le k \le n$. With the previous definitions*

$$u_n u_{k-1} = u_{n-1}u_k - (-1)^k a^k u_{n-k-1} \ .$$

Proof. By definition we can write

$$\begin{aligned} u_n u_{k-1} - u_{n-1}u_k &= \det \begin{pmatrix} u_n & u_k \\ u_{n-1} & u_{k-1} \end{pmatrix} \\ &= \det \left(M^k \begin{pmatrix} u_{n-k} & u_0 \\ u_{n-k-1} & u_{-1} \end{pmatrix} \right) \\ &= (\det M)^k \det \begin{pmatrix} u_{n-k} & 1 \\ u_{n-k-1} & 0 \end{pmatrix} \\ &= (-a)^k \left(-u_{n-k-1}\right) \ , \end{aligned}$$

which proves the lemma. □

Lemma 6.2. *Let $0 < k \le n$ and u_n as before. Then*

$$u_n = u_{n-k}u_k + a u_{n-k-1}u_{k-1} \ .$$

Proof.
Let

$$U_{l-2} = \begin{pmatrix} u_l & a u_{l-1} \\ u_{l-1} & a u_{l-2} \end{pmatrix} \quad \text{for} \quad l = 1, 2, \dots \ .$$

Clearly,

$$U_{-1} = M \quad \text{and} \quad U_{l+1} = M U_l$$

whence

$$U_{k-2} = M^{k-1} U_{-1} = M^k \ .$$

Hence,

$$\bar{u}_{n-1} = M^k \bar{u}_{n-k-1} = U_{k-2}\bar{u}_{n-k-1} \ ,$$

what we had to prove. □

Corollary 6.3. *Let $n \ge 1$. Then*

$$u_{n+2} = u_3 u_n - a^2 u_{n-2} \ .$$

Proof. By Lemma 6.2,

$$u_{n+2} = u_2 u_n + a u_1 u_{n-1} \ .$$

Using the substitution

$$u_{n-1} = u_n - a u_{n-2} \ ,$$

we obtain

$$u_{n+2} = (u_2 + a u_1)u_n - a^2 u_1 u_{n-2} = u_3 u_n - a^2 u_{n-2} \ . \quad \square$$

Lemma 6.4. *Let R be a unique factorization domain, $n \in \mathbb{N}$ and let u be as above. Then*

$$\gcd(a, u_n) = 1 \ .$$

Proof. Let $m_i = \gcd(a, u_i)$. By the recurrence relation, we have

$$u_{i-1} = u_i - au_{i-2} \quad \text{for all} \quad i > 1 \ ,$$

whence

$$m_i \mid u_{i-1} \quad \text{for all} \quad i > 2$$

and thus

$$m_i \mid m_{i-1} \quad \text{for all} \quad i > 2 \ .$$

This yields that

$$\gcd(a, u_n) = m_n \mid m_1 = \gcd(a, u_1) \mid u_1 = 1 \ ,$$

whence $\gcd(a, u_i) = 1$. □

Lemma 6.5. *Let R, n and u be as in Lemma 6.4. Then*

$$\gcd(u_{n+1}, u_n) = 1 \ .$$

Proof. Let $m_i = \gcd(u_i, u_{i-1})$. Similarly, as in the proof of Lemma 6.4, we have

$$au_{i-2} = u_i - u_{i-1} \quad \text{for all} \quad i > 1 \ ,$$

whence $m_i \mid au_{i-2}$.

By Lemma 6.4, $\gcd(a, m_i) = 1$, thus $m_i \mid u_{i-2}$. This yields that

$$m_i \mid \gcd(u_{i-1}, u_{i-2}) = m_{i-1} \quad \text{for all} \quad i > 1 \ ,$$

whence

$$\gcd(u_{n+1}, u_n) = m_{n+1} \mid m_1 = \gcd(u_1, u_0) = 1 \ ,$$

thus $m_{n+1} = 1$. □

Lemma 6.6. *Let R be a unique factorization domain, $n, k \geq 1$ and u is a linear recurring sequence, defined as above, and suppose that $m = \gcd(n, k)$. Then*

$$\gcd\left(u_{n-1}, u_{k-1}\right) = u_{m-1} \ .$$

Proof. Without loss of generality, we may assume that $k \leq n$.

Let

$$n_0 = n \ , \quad k_0 = k$$

and

$$n_{i+1} = \max\{n_i - k_i, k_i\} \ , \quad k_{i+1} = \min\{n_i - k_i, k_i\} \quad \text{for} \quad i \geq 0 \ .$$

Clearly, $n_{i+1} < n_i$, thus there exists $j \in \mathbb{N}$, such that $n_j > 0$ but $n_{j+1} = 0$ and for this j, $n_j = k_j$. Furthermore, if $n_i > 0$, then $\gcd(n_i, k_i) = m$, whence $m = n_j$.

By Lemma 6.1,

$$u_{n_i-1}u_{k_i-2} = u_{n_i-2}u_{k_i-1} - (-1)^{k_i-1}a^{k_i-1}u_{n_i-k_i-1} \ , \tag{6.1}$$

whence

$$\gcd(u_{n_i-1}, u_{k_i-1}) \mid a^{k_i-1}u_{n_i-k_i-1}$$

and by Lemma 6.4,

$$\gcd(a, u_{k_i-1}) = 1 \ ,$$

thus

$$\gcd(u_{n_i-1}, u_{k_i-1}) \mid u_{n_i-k_i-1} \ .$$

Similarly, by (6.1) ,

$$\gcd(u_{k_i-1}, u_{n_i-k_i-1}) \mid u_{n_i-1}u_{k_i-2}$$

and by Lemma 6.5,

$$\gcd\left(u_{k_i-1}, u_{k_i-2}\right) = 1 \ ,$$

whence

$$\gcd(u_{k_i-1}, u_{n_i-k_i-1}) \mid u_{n_i-1} \ .$$

These all together yield that

$$\gcd(u_{n_i-1}, u_{k_i-1}) = \gcd(u_{k_i-1}, u_{n_i-k_i-1}) = \gcd(u_{n_{i+1}-1}, u_{k_{i+1}-1}) \ .$$

Hence

$$\gcd(u_{n-1}, u_{k-1}) = \gcd(u_{n_0-1}, u_{k_0-1}) = \gcd(u_{n_j-1}, u_{k_j-1}) = u_{n_j-1} = u_{m-1} \ . \quad \square$$

Lemma 6.7. *Let R be an integral domain and let u be a second-order linear recurring sequence over R satisfying the recurrence relation*

$$u_{n+2} = au_{n+1} + bu_n \quad \textit{for all} \quad n \in \mathbb{N} \ .$$

Suppose that the characteristic polynomial $x^2 - ax - b$ of u splits into linear factors over R and has no multiple roots. Suppose further, that $(\alpha_1 - \alpha_2)^{-1} \in R$, where α_1 and α_2 are the two different roots of $x^2 - ax - b$.

Then

$$u_n = d_1\alpha_1^n + d_2\alpha_2^n \quad \textit{for all} \quad n \in \mathbb{N} \ ,$$

where $d_1, d_2 \in R$ depend only on u_0 and u_1.

Proof. With the conditions of the Lemma, the system of linear equations

$$\begin{aligned} u_0 &= \quad d_1 + \quad d_2 \\ u_1 &= \alpha_1 d_1 + \alpha_2 d_2 \end{aligned}$$

has a solution in R, namely

$$d_1 = -\frac{\alpha_2 u_0 - u_1}{\alpha_1 - \alpha_2}$$
$$d_2 = \frac{\alpha_1 u_0 - u_1}{\alpha_1 - \alpha_2} \quad .$$

Let $n \in \mathbb{N}$, $d_1, d_2 \in R$ and suppose that

$$u_k = d_1\alpha_1^k + d_2\alpha_2^k \quad \text{for all} \quad 0 \leq k < n \ .$$

Since α_1 and α_2 are roots of $x^2 - ax - b$, thus

$$\alpha_1^2 = a\alpha_1 + b \quad \text{and} \quad \alpha_1^2 = a\alpha_1 + b \ .$$

Hence,

$$\begin{aligned} u_n &= au_{n-1} + bu_{n-2} \\ &= ad_1\alpha_1^{n-1} + d_2\alpha_2^{n-1} + bd_1\alpha_1^{n-2} + d_2\alpha_2^{n-2} \\ &= d_1\alpha_1^{n-2}(a\alpha_1 + b) + d_2\alpha_2^{n-2}(a\alpha_2 + b) \\ &= d_1\alpha_1^{n-2}\alpha_1^2 + d_2\alpha_2^{n-2}\alpha_2^2 \\ &= d_1\alpha_1^n + d_2\alpha_2^n \ . \end{aligned}$$

By induction we obtain the lemma. □

Remark 6.8. *If R is an integral domain, but does not contain any of the required elements in Lemma 6.7, then we can work in a proper R' extension of R, instead.*

Further on, let $F_n(x)$ be the sequence of polynomials over $\mathbb{Z}$ satisfying the recurrence relation

$$F_n(x) = F_{n-1}(x) + x \cdot F_{n-2}(x) \quad \text{for} \quad n \geq 2$$

with initial values $F_0(x) = F_1(x) = 1$.

Remark 6.9. *Some of the first few elements of the sequence are:*

$F_0(x) = 1$	$F_1(x) = 1$
$F_2(x) = x + 1$	$F_3(x) = 2x + 1$
$F_4(x) = x^2 + 3x + 1$	$F_5(x) = 3x^2 + 4x + 1$
$F_6(x) = x^3 + 6x^2 + 5x + 1$	$F_7(x) = 4x^3 + 10x^2 + 6x + 1$
$F_8(x) = x^4 + 10x^3 + 15x^2 + 7x + 1$	$F_9(x) = 5x^4 + 20x^3 + 21x^2 + 8x + 1$

Lemma 6.10. *Let $n \in \mathbb{N}$. With the previous definition of $F_n(x)$ we have*

$$\deg\left(F_n(x)\right) = \left[\frac{n}{2}\right] \ .$$

Proof. By definition, $F_0(x) = F_1(x) = 1$, thus

$$\deg\left(F_0(x)\right) = \left[\frac{0}{2}\right] \quad \text{and} \quad \deg\left(F_1(x)\right) = \left[\frac{1}{2}\right] \ .$$

Let $n \geq 2$ and suppose that

$$\deg\left(F_k(x)\right) = \left[\frac{k}{2}\right] \quad \text{if} \quad k < n \ .$$

In the recurrence relation of $F_n(x)$ there are only addition and multiplication, thus the leading coefficient of $F_k(x)$ is positive, whence

$$\begin{aligned}
\deg\left(F_n(x)\right) &= \deg\left(F_{n-1}(x) + x \cdot F_{n-2}(x)\right) \\
&= \max\left\{\deg\left(F_{n-1}(x)\right), \deg\left(F_{n-2}(x)\right) + 1\right\} \\
&= \max\left\{\left[\frac{n-1}{2}\right], \left[\frac{n-2}{2}\right] + 1\right\} \\
&= \left[\frac{n}{2}\right] \ . \qquad \square
\end{aligned}$$

Lemma 6.11. *The leading coefficient of $F_n(x)$ is*

$$\mathrm{lc}(F_n) = \begin{cases} 1 \ \textit{if } n = 2k \\ k+1 \ \textit{if } n = 2k+1 \end{cases}$$

with some $k \in \mathbb{N}$.

Proof. By Lemma 6.10,

$$\deg(F_{n+2}) = 1 + \deg(F_n) = 2 + \deg(F_{n-2})$$

and clearly

$$\mathrm{lc}(F_0) = \mathrm{lc}(F_2) = 1 \ .$$

Suppose that $n \geq 4$ is even and

$$\mathrm{lc}(F_{n-2}) = \mathrm{lc}(F_{n-4}) = 1 \ .$$

By Corollary 6.3,

$$F_n(x) = (2x+1)F_{n-2}(x) - x^2 F_{n-4}(x) \ .$$

Since

$$\deg((2x+1)F_{n-2}(x)) = \deg(x^2 F_{n-4}(x)) \ ,$$

$$\mathrm{lc}((2x+1)F_{n-2}(x)) = 2$$

and

$$\mathrm{lc}(x^2 F_{n-4}(x)) = 1 \ ,$$

thus

$$\mathrm{lc}(F_n(x)) = 1 \ .$$

Hence

$$\mathrm{lc}(F_n) = 1 \quad \text{for all even} \quad n \ .$$

Obviously,

$$\mathrm{lc}(F_1) = 1 \quad \text{and} \quad \mathrm{lc}(F_3) = 2 \ .$$

Suppose now that $n \geq 5$ is odd,

$$\mathrm{lc}(F_{n-2}) = \left[\frac{n-2}{2}\right] + 1 \quad \text{and} \quad \mathrm{lc}(F_{n-4}) = \left[\frac{n-4}{2}\right] + 1 \ ,$$

i.e.

$$\mathrm{lc}(F_{n-2}) = \mathrm{lc}(F_{n-4}) + 1 \ .$$

Similarly as above, we can write

$$\mathrm{lc}((2x+1)F_{n-2}(x)) = 2(\mathrm{lc}(F_{n-4}(x)) + 1)$$

and

$$\mathrm{lc}(x^2 F_{n-4}(x)) = \mathrm{lc}(F_{n-4}(x)) \ ,$$

whence

$$\begin{aligned} \mathrm{lc}(F_n(x)) &= 2(\mathrm{lc}(F_{n-4}(x)) + 1) - \mathrm{lc}(F_{n-4}(x))) \\ &= \mathrm{lc}(F_{n-4}(x))) + 2 \\ &= \left[\frac{n-4}{2}\right] + 3 = \left[\frac{n}{2}\right] + 1 \ . \end{aligned}$$

This proves that

$$\mathrm{lc}(F_n) = \left[\frac{n}{2}\right] + 1 \quad \text{for all odd} \quad n\text{'s} \ . \quad \square$$

Lemma 6.12. *The roots of $F_n(x)$ are*

$$-\frac{\xi_{n+1}^j}{\left(\xi_{n+1}^j + 1\right)^2} \ ,$$

where $1 \leq j \leq \left[\frac{n}{2}\right]$ and ξ_{n+1} is an $n+1$-th primitive root of unity.

Proof. Let

$$r, s \in \mathbb{Z} \setminus \{0\} \quad \text{with} \quad r^2 + 4s \neq 0$$

and u_m be a sequence of integers satisfying the recurrence relation

$$u_m = r u_{m-1} + s u_{m-2} \ ,$$

such that $|u_0| + |u_1| > 0$. Then by Lemma 6.7,

$$u_m = a \cdot \alpha^m + b \cdot \beta^m \quad \text{for all} \quad m \in \mathbb{N} \ ,$$

where α, β are the two different roots of the polynomial $z^2 - r \cdot z - s$ (in the proper extension of $\mathbb{Q}$) and

$$a = \frac{u_0 \cdot \beta - u_1}{\beta - \alpha} \ , \quad b = \frac{u_1 - u_0 \cdot \alpha}{\beta - \alpha} \ .$$

Suppose now that t is a root of $F_n(x)$ and define u_m by the following:

$$u_m = u_{m-1} + t \cdot u_{m-2} \quad \text{for} \quad m \geq 2$$

with initial values $u_0 = u_1 = 1$. It is clear that

$$F_m(t) = u_m \qquad \text{for } m \in \mathbb{N}$$

and if $t \neq -\frac{1}{4}$, then

$$\begin{aligned} u_m &= \frac{\sqrt{1+4t}-1}{2\sqrt{1+4t}} \cdot \left(\frac{1-\sqrt{1+4t}}{2}\right)^m + \frac{\sqrt{1+4t}+1}{2\sqrt{1+4t}} \cdot \left(\frac{1+\sqrt{1+4t}}{2}\right)^m \\ &= \frac{1}{\sqrt{1+4t}} \cdot \left(\left(\frac{1+\sqrt{1+4t}}{2}\right)^{m+1} - \left(\frac{1-\sqrt{1+4t}}{2}\right)^{m+1}\right) \ . \end{aligned}$$

By the choice of t we have $0 = F_n(t) = u_n$, which yields

$$\left(\frac{1+\sqrt{1+4t}}{2}\right)^{n+1} - \left(\frac{1-\sqrt{1+4t}}{2}\right)^{n+1} = 0 \ ,$$

i.e.

$$\left(\frac{1+\sqrt{1+4t}}{2}\right)^{n+1} = \left(\frac{1-\sqrt{1+4t}}{2}\right)^{n+1} \ .$$

Hence

$$\left(1+\sqrt{1+4t}\right) = \xi_{n+1}^j \cdot \left(1-\sqrt{1+4t}\right)$$

for some j and ξ_{n+1}, where ξ_{n+1} is an $n+1$-th primitive root of unity and $1 \leq j \leq n$. Solving the equation we obtain

$$t = -\frac{\xi_{n+1}^j}{\left(\xi_{n+1}^j + 1\right)^2} \ .$$

Observing the possible values of t we find the followings:

(i) $j \neq \frac{n+1}{2}$ (if $\frac{n+1}{2}$ is integer at all), otherwise

$$1 + \sqrt{1+4t} = \xi_{n+1}^j \cdot \left(1-\sqrt{1+4t}\right) = \sqrt{1+4t} - 1$$

would hold, which is impossible.

(ii) In the case $j = 0$ we have $t = -\frac{1}{4}$ and the corresponding recurring sequence $u_m = \frac{m+1}{2^m}$. This would yield that

$$0 = F_n\left(-\frac{1}{4}\right) = u_n = \frac{n+1}{2^n} \neq 0 \ ,$$

which is a contradiction.

(iii) If $0 \leq i, j < n+1$ and $i \neq j$, then

$$-\frac{\xi_{n+1}^i}{\left(\xi_{n+1}^i + 1\right)^2} = -\frac{\xi_{n+1}^j}{\left(\xi_{n+1}^j + 1\right)^2}$$

if and only if $i + j = n + 1$. Indeed,

$$-\frac{\xi_{n+1}^i}{\left(\xi_{n+1}^i + 1\right)^2} = -\frac{\xi_{n+1}^j}{\left(\xi_{n+1}^j + 1\right)^2}$$

if and only if

$$0 = \frac{\xi_{n+1}^i}{\left(\xi_{n+1}^i + 1\right)^2} - \frac{\xi_{n+1}^j}{\left(\xi_{n+1}^j + 1\right)^2} = \frac{\xi_{n+1}^i\left(\xi_{n+1}^j + 1\right)^2 - \xi_{n+1}^j\left(\xi_{n+1}^i + 1\right)^2}{\left(\xi_{n+1}^i + 1\right)^2\left(\xi_{n+1}^j + 1\right)^2} \ ,$$

which is equivalent to

$$\begin{aligned}
&\xi_{n+1}^i\left(\xi_{n+1}^j + 1\right)^2 - \xi_{n+1}^j\left(\xi_{n+1}^i + 1\right)^2 \\
&\quad = \xi_{n+1}^i\xi_{n+1}^{2j} + 2\xi_{n+1}^i\xi_{n+1}^j + \xi_{n+1}^i - \xi_{n+1}^j\xi_{n+1}^{2i} + 2\xi_{n+1}^j\xi_{n+1}^i + \xi_{n+1}^j \\
&\quad = \xi_{n+1}^i\xi_{n+1}^j\left(\xi_{n+1}^j - \xi_{n+1}^i\right) + \xi_{n+1}^i - \xi_{n+1}^j \\
&\quad = \left(\xi_{n+1}^i\xi_{n+1}^j - 1\right)\left(\xi_{n+1}^j - \xi_{n+1}^i\right) \\
&\quad = 0 \ .
\end{aligned}$$

Since $i \neq j$, the above can hold if and only if

$$\xi_{n+1}^i\xi_{n+1}^j - 1 = 0 \ ,$$

which proves our claim.

This yields that the values

$$t_1 = -\frac{\xi_{n+1}}{\left(\xi_{n+1} + 1\right)^2}$$

$$\vdots$$

$$t_{\left[\frac{n}{2}\right]} = -\frac{\xi_{n+1}^{\left[\frac{n}{2}\right]}}{\left(\xi_{n+1}^{\left[\frac{n}{2}\right]} + 1\right)^2}$$

are all different and by definition,

$$F_n(t_j) = 0 \quad \text{for all} \quad 1 \le j \le \left[\frac{n}{2}\right] \ .$$

Since

$$\deg\left(F_n(x)\right) = \left[\frac{n}{2}\right] \ ,$$

we have

$$F_n(x) = \prod_{j=1}^{\left[\frac{n}{2}\right]} \left(x + \frac{\xi_{n+1}^j}{\left(\xi_{n+1}^j + 1\right)^2} \right) \ . \quad \square$$

Remark 6.13. *The complex conjugate of the numbers ξ_{n+1}^j are ξ_{n+1}^{n+1-j}, whence by the proof of Lemma 6.2 we find that the complex conjugate of $-\frac{\xi_{n+1}^j}{\left(\xi_{n+1}^j+1\right)^2}$ is itself. This yields that all the roots of $F_n(x)$ are real.*

Remark 6.14. *It is clear from the proof of Lemma 6.12, that all the roots of $F_n(x)$ are different.*

Remark 6.15. *Since $0 < j < \left[\frac{n+1}{2}\right]$, thus $\xi_{n+1}^j \notin \mathbb{R}$, in particular, $\xi_{n+1}^j \notin \{-1, 1\}$. Hence*

$$\left|\xi_{n+1}^j + 1\right| < \left|\xi_{n+1}^j\right| + 1 = 2 \ , \tag{6.2}$$

the sum of the conjugates, $\xi_{n+1}^j + \xi_{n+1}^{-j}$ are real and

$$\left|\xi_{n+1}^j + \xi_{n+1}^{-j}\right| < \left|\xi_{n+1}^j\right| + \left|\xi_{n+1}^{-j}\right| = 2 \ . \tag{6.3}$$

Furthermore, the difference of the conjugates, $\xi_{n+1}^{-j} - \xi_{n+1}^j \neq 0$ and is purely imaginary, whence

$$\left(\xi_{n+1}^{-j} - \xi_{n+1}^j\right)^2 \in \mathbb{R}^- \ . \tag{6.4}$$

The inequality (6.2) *implies that*

$$\left|\frac{\xi_{n+1}^j}{\left(\xi_{n+1}^j + 1\right)^2}\right| = \frac{\left|\xi_{n+1}^j\right|}{\left|\left(\xi_{n+1}^j + 1\right)^2\right|} = \frac{1}{\left(\left|\xi_{n+1}^j + 1\right|\right)^2} > \frac{1}{4} \ . \tag{6.5}$$

By (6.3) *and* (6.4) *we have*

$$\frac{\xi_{n+1}^j}{\left(\xi_{n+1}^j + 1\right)^2} = \frac{\xi_{n+1}^j}{\left(\xi_{n+1}^j + 1\right)^2} \cdot \frac{\left(\xi_{n+1}^{-j} - 1\right)^2}{\left(\xi_{n+1}^{-j} - 1\right)^2} = \frac{\xi_{n+1}^j + \xi_{n+1}^{-j} - 2}{\left(\xi_{n+1}^{-j} - \xi_{n+1}^j\right)^2} < 0 \quad .$$

This and (6.5) *together yield that all the roots of $F_n(x)$ are less than $-\frac{1}{4}$. Consequently, since the leading coefficients of $F_n(x)$ are positive, thus*

$$0 < F_n\left(-\frac{1}{4}\right) \le F_n\left(x_1\right) \le F_n\left(x_2\right) \quad \textit{for all} \quad -\frac{1}{4} \le x_1 \le x_2 \ .$$

Remark 6.16. *Let u_n be the sequence defined by the recurrence relation*

$$u_n = u_{n-1} - \frac{1}{4}u_{n-2} \quad \textit{for} \quad n \geq 2 \ ,$$

with starting values $u_0 = u_1 = 1$.

Then

$$F_n\left(-\frac{1}{4}\right) = u_n \quad \textit{for all} \quad n \in \mathbb{N}$$

and

$$u_n = (c_1 n + c_2)\left(\frac{1}{2}\right)^n \quad \textit{for all} \quad n \in \mathbb{N}$$

with some $c_1, c_2 \in \mathbb{Q}$. (See e.g. Chapter C in [43].)

Solving the system of equations

$$\begin{aligned} 1 = u_0 = & \quad c_2 \\ 1 = u_1 = & \frac{1}{2}\, c_1 + \frac{1}{2}\, c_2 \ , \end{aligned}$$

we obtain that

$$F_n\left(-\frac{1}{4}\right) = u_n = (n+1)\left(\frac{1}{2}\right)^n \quad \textit{for all} \quad n \in \mathbb{N} \ .$$

Remark 6.17. *Let u_n be the sequence defined by the recurrence*

$$u_n = u_{n-1} + \frac{1}{4}u_{n-2} \quad \textit{for} \quad n \geq 2 \ ,$$

with starting values $u_0 = u_1 = 1$.

Then

$$F_n\left(\frac{1}{4}\right) = u_n = \frac{2+\sqrt{2}}{4}\left(\frac{1+\sqrt{2}}{2}\right)^n + \frac{2-\sqrt{2}}{4}\left(\frac{1-\sqrt{2}}{2}\right)^n \quad \textit{for all} \quad n \in \mathbb{N} \ .$$

Lemma 6.18. *Let $n \in \mathbb{N}$. With the previous definitions, $F_n(x)$ has a rational root if and only if* $\gcd(n+1, 12) \geq 3$ *and the rational roots of $F_n(x)$ are in the set $\{-1, -\frac{1}{2}, -\frac{1}{3}\}$.*

Proof. By Lemma 6.12, $F_n(x)$ has a rational root if and only if

$$-\frac{\xi_{n+1}^j}{\left(\xi_{n+1}^j + 1\right)^2} = \frac{p}{q} \tag{6.6}$$

for some $j \in \left\{1, 2, \ldots, \left[\frac{n}{2}\right]\right\}$ and $p, q \in \mathbb{Z}$, where $q \neq 0$.

Equation (6.6) is equivalent to

$$0 = p\left(\xi_{n+1}^j + 1\right)^2 + q\xi_{n+1}^j = p\left(\xi_{n+1}^j\right)^2 + (q+2p)\xi_{n+1}^j + p \ .$$

Hence ξ_{n+1}^j has to be a root of the polynomial

$$px^2 + (q+2p)x + p \ ,$$

which yields that ξ_{n+1}^j is rational or a quadratic algebraic number.

On the other hand, ξ_{n+1}^j is a root of unity and thus a primitive k-th root of unity, with some $k \in \mathbb{N}$. It is known that a primitive k-th root of unity has degree $\varphi(k)$, where $\varphi(k)$ is the Euler-function. By the basic properties of $\varphi(k)$, we can show that $\varphi(k) \le 2$ if and only if $k \in \{1,2,3,4,6\}$.

If ξ_{n+1}^j is a primitive first root of unity, then $\xi_{n+1}^j = 1$, but $j \in \left\{1, 2, \dots, \left[\frac{n}{2}\right]\right\}$, which is a contradiction.

Similarly, if ξ_{n+1}^j is a primitive second root of unity, then $\xi_{n+1}^j = -1$, but this can take place if and only if $2j = n+1$, which is, again, not possible.

It follows that, ξ_{n+1}^j can be a primitive $3, 4$ or 6-th root of unity only, and the corresponding values of t are $-1, -\frac{1}{2}$ and $-\frac{1}{3}$, respectively.

The algebraic number ξ_{n+1}^j is a primitive k-th root of unity if and only if

$$n+1 \mid jk \ , \quad \text{but} \quad n+1 \nmid jk' \quad \text{for any} \quad 1 \le k' < k \ ,$$

and this is true exactly when

$$n+1 = k \cdot \gcd(n+1, j) \ .$$

Thus $F_n(x)$ has a rational root if and only if

$$3 \mid n+1 \ , \quad 4 \mid n+1 \quad \text{or} \quad 6 \mid n+1 \ ,$$

i.e. $\gcd(n+1, 12) \ge 3$. $\square$

We will define the polynomial sequence $f_n(x,y)$ by the following relation:

$$f_n(x,y) = \begin{cases} y^{\left[\frac{n}{2}\right]} \cdot F_n\left(\frac{x}{y}\right) & \text{if } n \in \mathbb{N} \\ 0 & \text{if } n < 0 \ . \end{cases}$$

Remark 6.19. *By Lemma 6.12, we can see that $f_n(x,y)$ are really polynomials and not rational fractions.*

Remark 6.20. *With the previous definition*

$$\delta_{0n} \cdot f_n(x,y) = y^{\chi(n-1)} \cdot f_{n-1}(x,y) + x \cdot f_{n-2}(x,y) \quad \textit{for} \quad n \in \mathbb{Z} \ , \tag{6.7}$$

where

$$\delta_{0n} = \begin{cases} 0, & \textit{if } n = 0 \\ 1, & \textit{if } n \ne 0 \ . \end{cases}$$

Proof. Let $n \geq 2$. Then

$$\begin{aligned}\delta_{0n} \cdot f_n(x,y) &= f_n(x,y) \\ &= y^{\left[\frac{n}{2}\right]} \cdot F_n\left(\frac{x}{y}\right) \\ &= y^{\left[\frac{n}{2}\right]}\left(F_{n-1}\left(\frac{x}{y}\right) + \frac{x}{y}F_{n-2}\left(\frac{x}{y}\right)\right) \\ &= y^{\left[\frac{n}{2}\right]-\left[\frac{n-1}{2}\right]} \cdot f_{n-1}(x,y) + \frac{x}{y}y^{\left[\frac{n}{2}\right]-\left[\frac{n-2}{2}\right]} \cdot f_{n-2}(x,y)\ ,\end{aligned}$$

which is (6.7).

If $n = 1$, then (6.7) has the form

$$1 = y^0 \cdot 1 + x \cdot 0$$

and if $n = 0$, then (6.7) looks like

$$0 = y \cdot 0 + x \cdot 0\ ,$$

which is also true. If $n < 0$, then (6.7) obviously holds. □

Remark 6.21. *Replacing y by y^2 in the definition of $f_n(x,y)$ it is easy to prove that*

$$y^{\chi(n)} f_n(x,y^2) = y^n F_n\left(\frac{x}{y^2}\right)\ .$$

Lemma 6.22. *Let $n, k \in \mathbb{N}$, such that $n \geq k$. Then*

$$\begin{aligned}y^{\chi(n-1)} f_{n-1}\left(x,y^2\right) y^{\chi(k-2)} f_{k-2}\left(x,y^2\right) - y^{\chi(n-2)} f_{n-2}\left(x,y^2\right) y^{\chi(k-1)} f_{k-1}\left(x,y^2\right) \\ = (-1)^k\, x^{k-1} y^{2k-1} y^{\chi(n-k-1)} \cdot f_{n-k-1}\left(x,y^2\right)\ .\end{aligned}$$

Proof. By Remark 6.21 and Lemma 6.1,

$$\begin{aligned}&y^{\chi(n-1)} f_{n-1}\left(x,y^2\right) y^{\chi(k-2)} f_{k-2}\left(x,y^2\right) - y^{\chi(n-2)} f_{n-2}\left(x,y^2\right) y^{\chi(k-1)} f_{k-1}\left(x,y^2\right) \\ &\quad = y^{n-1} F_{n-1}\left(\frac{x}{y^2}\right) y^{k-2} F_{k-2}\left(\frac{x}{y^2}\right) - y^{n-2} F_{n-2}\left(\frac{x}{y^2}\right) y^{k-1} F_{k-1}\left(\frac{x}{y^2}\right) \\ &\quad = y^{n+k-2}(-1)^k x^{k-1} F_{n-k-1}\left(\frac{x}{y^2}\right) \\ &\quad = (-1)^k\, x^{k-1} y^{2k-1} y^{\chi(n-k-1)} \cdot f_{n-k-1}\left(x,y^2\right)\ .\quad \square\end{aligned}$$

Lemma 6.23. *Let $n, k \in \mathbb{N}$ and suppose that* $\gcd(n,k) = m$. *Then*

$$y^{\chi(m-1)} \cdot f_{m-1}\left(x, y^2\right) \mid y^{\chi(n-1)} \cdot f_{n-1}\left(x, y^2\right) \ .$$

(By symmetry, obviously the same holds, if we replace n by k.)

Proof. By Lemma 6.6,

$$F_{m-1} \mid F_{n-1} \quad \text{and} \quad F_{m-1} \mid F_{k-1} \ . \tag{6.8}$$

Let R be an integral domain, $l(x), P(x), Q(x), S(x) \in R[x]$, such that

$$P(x) = Q(x)S(x)$$

with degrees

$$\deg(P) = p \ , \quad \deg(Q) = q \quad \text{and} \quad \deg(S) = s \ .$$

Then we have

$$y^p P(\frac{l(x)}{y}),\ y^q Q(\frac{l(x)}{y}),\ y^s S(\frac{l(x)}{y}) \in R[x,y]$$

and since $p = q + s$, thus

$$y^p P(\frac{l(x)}{y}) = y^q Q(\frac{l(x)}{y}) \cdot y^s S(\frac{l(x)}{y}) \ .$$

Hence, by Remark 6.21 and (6.8) the Lemma follows. □

Lemma 6.24. *Let $n \geq 1$. Then*

$$f_{n+2}(x,y) = (2x+y) \cdot f_n(x,y) - x^2 \cdot f_{n-2}(x,y) \ .$$

Proof. By Corollary 6.3,

$$F_{n+2}(z) = F_3(z)F_n(z) - z^2 F_{n-2}(z) \ .$$

Substituting z by $\frac{x}{y}$ and multiplying both sides of the equation by $y^{\left[\frac{n+2}{2}\right]}$ we obtain

$$y^{\left[\frac{n+2}{2}\right]} F_{n+2}\left(\frac{x}{y}\right) = yF_3\left(\frac{x}{y}\right) y^{\left[\frac{n}{2}\right]} F_n\left(\frac{x}{y}\right) - y^2\left(\frac{x}{y}\right)^2 y^{\left[\frac{n-2}{2}\right]} F_{n-2}\left(\frac{x}{y}\right) \ ,$$

which is exactly what we had to prove. □

Lemma 6.25. *Let*

$$D = D(x,y) = y \cdot (4x+y) \ , \quad U_1 = U_1(x,y) = \frac{2x+y+\sqrt{D}}{2}$$

and

$$U_2 = U_2(x,y) = \frac{2x+y-\sqrt{D}}{2} \ .$$

Then

$$f_n(x,y) = \left(\frac{1}{2}\right)^{\chi(n+1)} \frac{\left(y+\sqrt{D}\right)^{\chi(n+1)} \cdot U_1^{\left[\frac{n+1}{2}\right]} - \left(y-\sqrt{D}\right)^{\chi(n+1)} \cdot U_2^{\left[\frac{n+1}{2}\right]}}{\sqrt{D}} \ .$$

Proof. Define the following subsequences of $f_n(x,y)$:

$$u_k = f_{2k} \quad \text{and} \quad v_k = f_{2k+1} \ .$$

By Lemma 6.24 we find

$$u_{k+2}(x,y) = (2x+y)u_{k+1}(x,y) - x^2 u_k(x,y)$$

and

$$v_{k+2}(x,y) = (2x+y)v_{k+1}(x,y) - x^2 v_k(x,y)$$

for all $k \in \mathbb{N}$. The characteristic polynomial of u and v is

$$z^2 - (2x+y)z + x^2 \ ,$$

which has the roots U_1 and U_2. Clearly,

$$\sqrt{D} = U_1 - U_2 \ , \quad u_0 = f_0 = 1 \ , \quad u_1 = f_2 = x+y \ ,$$
$$v_0 = f_1 = 1 \quad \text{and} \quad v_1 = f_3 = 2x+y \ .$$

Applying Lemma 6.7, we obtain

$$\begin{aligned} u_k &= -\frac{U_2 u_0 - u_1}{U_1 - U_2} U_1^k + \frac{U_1 u_0 - u_1}{U_1 - U_2} U_2^k \\ &= -\frac{\frac{2x+y-\sqrt{D}}{2} - (x+y)}{\sqrt{D}} U_1^k + \frac{\frac{2x+y+\sqrt{D}}{2} - (x+y)}{\sqrt{D}} U_2^k \\ &= -\frac{1}{2} \frac{2x+y-\sqrt{D}-2x-2y}{\sqrt{D}} U_1^k + \frac{1}{2} \frac{2x+y+\sqrt{D}-2x-2y}{\sqrt{D}} U_2^k \\ &= \frac{1}{2} \frac{y+\sqrt{D}}{\sqrt{D}} U_1^k - \frac{1}{2} \frac{y-\sqrt{D}}{\sqrt{D}} U_2^k \quad . \end{aligned}$$

Doing likewise, we have

$$\begin{aligned} v_k &= -\frac{U_2v_0 - v_1}{U_1 - U_2}U_1^k + \frac{U_1v_0 - v_1}{U_1 - U_2}U_2^k \\ &= -\frac{\frac{2x+y-\sqrt{D}}{2} - (2x+y)}{\sqrt{D}}U_1^k + \frac{\frac{2x+y+\sqrt{D}}{2} - (2x+y)}{\sqrt{D}}U_2^k \\ &= -\frac{\frac{1}{2}(2x+y-\sqrt{D}-4x-2y)}{\sqrt{D}}U_1^k + \frac{\frac{1}{2}(2x+y+\sqrt{D}-4x-2y)}{\sqrt{D}}U_2^k \\ &= \frac{\frac{1}{2}(2x+y+\sqrt{D})}{\sqrt{D}}U_1^k - \frac{\frac{1}{2}(2x+y-\sqrt{D})}{\sqrt{D}}U_2^k \\ &= \frac{1}{\sqrt{D}}U_1^{k+1} - \frac{1}{\sqrt{D}}U_2^{k+1} \quad . \end{aligned}$$

Since

$$f_n = \begin{cases} u_{\frac{n}{2}} & \text{if } n \text{ is even} \\ v_{\frac{n-1}{2}} & \text{if } n \text{ is odd} \end{cases} ,$$

thus substituting the formulas we obtained for u and v, we arrive to the statement of the Lemma. □

Remark 6.26. *The result of Lemma 6.25 can be formulated as follows: if n is odd, then*

$$f_n(x,y) = \frac{U_1^{\frac{n+1}{2}} - U_2^{\frac{n+1}{2}}}{\sqrt{D}} = \frac{U_1 - U_2}{\sqrt{D}} \sum_{i=0}^{\frac{n-1}{2}} U_1^i U_2^{\frac{n-1}{2}-i} = \sum_{i=0}^{\frac{n-1}{2}} U_1^i U_2^{\frac{n-1}{2}-i} ,$$

or else, if n is even, then

$$\begin{aligned} f_n(x,y) &= \frac{1}{2}\frac{\left(y+\sqrt{D}\right)\cdot U_1^{\frac{n}{2}} - \left(y-\sqrt{D}\right)\cdot U_2^{\frac{n}{2}}}{\sqrt{D}} \\ &= \frac{1}{2}U_1^{\frac{n}{2}} + \frac{1}{2}U_2^{\frac{n}{2}} + \frac{y}{2}\frac{U_1^{\frac{n}{2}} - U_2^{\frac{n}{2}}}{\sqrt{D}} \\ &= \frac{1}{2}U_1^{\frac{n}{2}} + \frac{1}{2}U_2^{\frac{n}{2}} + \frac{y}{2}\sum_{i=0}^{\frac{n}{2}-1} U_1^i U_2^{\frac{n}{2}-1-i} . \end{aligned}$$

This form has a special role, when we substitute x by $\hat{x}$ and y by $\hat{y}$, such that

$$\hat{y}\cdot(4\hat{x}+\hat{y}) = 0 .$$

In this case $U_1 = U_2$ and

$$f_n(\hat{x},\hat{y}) = \frac{n+1}{2}U_1^{\frac{n-1}{2}} \qquad \text{if } n \text{ is odd,}$$

and

$$f_n(\hat{x},\hat{y}) = U_1^{\frac{n}{2}} + \hat{y}\frac{n}{4}U_1^{\frac{n}{2}-1} \qquad \text{if } n \text{ is even.}$$

Combining the above formulas, we obtain

$$f_n(\hat{x},\hat{y}) = \left(\frac{2U_1}{n} + \frac{\hat{y}}{2}\right)^{\chi(n+1)} \left[\frac{n+1}{2}\right] U_1^{\left[\frac{n}{2}\right]} .$$

Lemma 6.27. *Let $A, B \in \mathbb{Z}$, such that $A^2 \neq iB$ where $i = 1,2,3,4$ and let α and β the roots of the polynomial $x^2 - Ax - B$. Then α/β is not a root of unity.*

Proof. See the Remarks on page 7 in [34].

Lemma 6.28. *Let u_n be a second-order linear recurring sequence, with two different roots of its characteristic polynomial, α and β. Suppose that $|\alpha| \geq |\beta|$, α/β is not a root of unity and u_n has no first-order recurrence relation. Then, there exists an effectively computable constant c_1 depending on u_n, such that*

$$|u_n| \geq |\alpha|^{n - c_1 \log n} .$$

Proof. The lemma is a simplified form of Theorem 3.1. of [43].

Lemma 6.29. *Let $\hat{x}, \hat{y} \in \mathbb{Z}$, such that $\hat{x} < -1$, $\hat{y} > 0$ and $4\hat{x} + \hat{y} < 0$ and suppose that $n > c_1$, where c_1 is effectively computable and depends only on $\hat{x}$ and $\hat{y}$.*

With the notation of Lemma 6.25, we have

$$f_n(\hat{x},\hat{y}) > 2^{\frac{n}{4}} .$$

Proof. Substituting x by $\hat{x}$ and y by $\hat{y}$ in Lemma 6.25, we obtain that

$$D(\hat{x},\hat{y}) < 0 ,$$

whence

$$|U_1(\hat{x},\hat{y})| = |U_2(\hat{x},\hat{y})| .$$

Since

$$U_1(\hat{x},\hat{y}) \cdot U_2(\hat{x},\hat{y}) = \hat{x}^2 ,$$

thus

$$|U_1(\hat{x},\hat{y})| = |\hat{x}| > 1 .$$

By Lemma 6.27, $U_1(\hat{x},\hat{y})/U_2(\hat{x},\hat{y})$ is not a root of unity, whence by Lemma 6.28 and Lemma 6.25, we obtain

$$f_n(\hat{x},\hat{y}) > |U_1(\hat{x},\hat{y})|^{\left[\frac{n+1}{2}\right] - c(\hat{x},\hat{y}) \cdot \log\left(\left[\frac{n+1}{2}\right]\right)} ,$$

where $c(\hat{x},\hat{y})$ is effective and depends only on $\hat{x}$ and $\hat{y}$.

If

$$n > 8 \cdot (c(\hat{x},\hat{y}))^2 + 1 ,$$

then

$$\left[\frac{n+1}{2}\right] - 2 \cdot c(\hat{x},\hat{y})\sqrt{\left[\frac{n+1}{2}\right]} > 0 \ .$$

Furthermore, if $a > e^2$, then $\sqrt{a} > \log a$, thus if

$$n > 8 \cdot (c(\hat{x},\hat{y}))^2 + 2e^2 \ ,$$

then

$$\left[\frac{n+1}{2}\right] > 2 \cdot c(\hat{x},\hat{y})\sqrt{\left[\frac{n+1}{2}\right]} > 2 \cdot c(\hat{x},\hat{y}) \log(\left[\frac{n+1}{2}\right]) \ .$$

Hence, using that $|U_1(\hat{x},\hat{y})| \geq 2$, we obtain

$$\begin{aligned} f_n(\hat{x},\hat{y}) &> |U_1(\hat{x},\hat{y})|^{\left[\frac{n+1}{2}\right] - c(\hat{x},\hat{y}) \cdot \log(\left[\frac{n+1}{2}\right])} \\ &> |U_1(\hat{x},\hat{y})|^{\frac{\left[\frac{n+1}{2}\right]}{2}} \\ &> |U_1(\hat{x},\hat{y})|^{\frac{n}{4}} \\ &> 2^{\frac{n}{4}} \ . \quad \square \end{aligned}$$

The following lemma generalizes a result of Ribenboim [38] and is basic for the proofs of the theorems.

Lemma 6.30. *Let $n \geq 2$, $1 \leq k < n$ and $a, b, A, B \in \mathbb{Z}$. If $x^2 - bx - a$ divides $x^n - Bx^k - A$, then*

$$B \cdot b^{\chi(k-1)} \cdot f_{k-1}\left(a, b^2\right) = b^{\chi(n-1)} \cdot f_{n-1}\left(a, b^2\right) \ ,$$

and

$$A = a \cdot \left(b^{\chi(n-2)} \cdot f_{n-2}\left(a, b^2\right) - B \cdot b^{\chi(k-2)} \cdot f_{k-2}\left(a, b^2\right)\right) \ .$$

Proof. Assume that

$$x^n - Bx^k - A = \left(x^2 - bx - a\right) \cdot p(x)$$

with

$$p(x) = x^{n-2} + c_{n-3}x^{n-3} + c_{n-4}x^{n-4} + \cdots + c_1 x + c_0 \ .$$

Then we have the following equations:

$$\begin{aligned} A &= a \cdot c_0 \\ \delta_{1,k} \cdot B &= a \cdot c_1 + b \cdot c_0 \\ &\vdots \\ \delta_{i,k} \cdot B &= a \cdot c_i + b \cdot c_{i-1} - c_{i-2} \\ &\vdots \\ \delta_{n-2,k} \cdot B &= a + b \cdot c_{n-3} - c_{n-4} \\ \delta_{n-1,k} \cdot B &= b - c_{n-3} \end{aligned} \tag{6.9}$$

where

$$\delta_{i,j} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{otherwise .} \end{cases}$$

First, we prove that if $1 \leq i \leq n-2$, then

$$c_{n-2-i} = b^{\chi(i)} \cdot f_i\left(a, b^2\right) - B \cdot b^{\chi(k-n+i)} \cdot f_{k-n+i}\left(a, b^2\right) \ . \tag{6.10}$$

If $i = 1$, then $f_i(x, y) = 1$ and since $k < n$, thus

$$f_{k-n+i}(x, y) = \delta_{n-1,k} \ .$$

Hence (6.10) yields

$$c_{n-2-1} = b \cdot 1 - B \cdot b^{\chi(k-n+1)} \cdot \delta_{n-1,k} \ ,$$

i.e.

$$c_{n-3} = \begin{cases} b & \text{if } k < n-1 \\ b - B & \text{if } k = n-1 \ , \end{cases}$$

which is true by (6.9).

If $i = 2$, then by Lemma 6.5,

$$f_i(x, y) = x + y$$

and (6.10) yields

$$c_{n-2-2} = a + b^2 - Bb^{\chi(k-n+i)} \cdot f_{k-n+i}\left(a, b^2\right) \ ,$$

i.e.

$$c_{n-4} = \begin{cases} a + b^2 & \text{if } k < n-2 \\ a + b^2 - B & \text{if } k = n-2 \\ a + b^2 - Bb & \text{if } k = n-1 \ . \end{cases}$$

Substituting the values c_{n-3} and c_{n-4} into (6.9), we find (6.10) correct again.

Now, let $2 < i \leq n-2$ and suppose that (6.10) holds for every j with $1 \leq j < i$. By (6.9) we can write

$$\begin{aligned} c_{n-2-i} &= a \cdot c_{n-2-(i-2)} + b \cdot c_{n-2-(i-1)} - \delta_{n-i,k} \cdot B \\ &= a \cdot C_1 + b \cdot C_2 - \delta_{n-i,k} \cdot B \\ &= b^{\chi(i-2)} \cdot C_3 - B \cdot b^{\chi(k-n+i-2)} \cdot C_4 + B \cdot \delta_{n-i,k} \ , \end{aligned} \tag{6.11}$$

where

$$\begin{aligned} C_1 &= b^{\chi(i-2)} \cdot f_{i-2}\left(a, b^2\right) - B \cdot b^{\chi(k-n+i-2)} \cdot f_{k-n+i-2}\left(a, b^2\right) \\ C_2 &= b^{\chi(i-1)} \cdot f_{i-1}\left(a, b^2\right) - B \cdot b^{\chi(k-n+i-1)} \cdot f_{k-n+i-1}\left(a, b^2\right) \\ C_3 &= b^{2(\chi(i-1))} \cdot f_{i-1}\left(a, b^2\right) + a \cdot f_{i-2}\left(a, b^2\right) \\ C_4 &= b^{2(\chi(k-n+i-1))} \cdot f_{k-n+i-1}\left(a, b^2\right) + a \cdot f_{k-n+i-2}\left(a, b^2\right) \ . \end{aligned}$$

By Lemma 6.5,

$$C_3 = f_i(a, b^2) \quad \text{and} \quad C_4 = f_{n-k}(a, b^2) \ .$$

Substituting C_3 and C_4 into (6.11), we obtain (6.10).

By (6.9) and (6.10) we have

$$\begin{aligned} 0 &= a \cdot c_1 + b \cdot c_0 - \delta_{1,k} \cdot B \\ &= a \cdot \left(b^{\chi(n-3)} \cdot f_{n-3}\left(a, b^2\right) - B \cdot b^{\chi(k-3)} \cdot f_{k-3}\left(a, b^2\right) \right) \\ &\quad + b \cdot a \cdot \left(b^{\chi(n-2)} \cdot f_{n-2}\left(a, b^2\right) - B \cdot b^{\chi(k-2)} \cdot f_{k-2}\left(a, b^2\right) \right) - \delta_{1,k} \cdot B \\ &= b^{\chi(n-3)} \cdot \left(b^{2\chi(n-2)} \cdot f_{n-2}\left(a, b^2\right) + a \cdot f_{n-3}\left(a, b^2\right) \right) \\ &\quad - B \cdot \left(b^{\chi(k-3)} \cdot \left(b^{2\chi(k-2)} \cdot f_{k-2}\left(a, b^2\right) + a \cdot f_{k-3}\left(a, b^2\right) \right) + \delta_{1,k} \right) \ , \end{aligned}$$

whence by Lemma 6.5, we come to

$$0 = b^{\chi(n-1)} \cdot f_{n-1}\left(a, b^2\right) - B \cdot b^{\chi(k-1)} \cdot f_{k-1}\left(a, b^2\right) \ ,$$

what we had to prove.

By simple substitution of (6.10) into (6.9), we get

$$A = a \cdot \left(b^{\chi(n-2)} \cdot f_{n-2}\left(a, b^2\right) - B \cdot b^{\chi(k-2)} \cdot f_{k-2}\left(a, b^2\right) \right) \ ,$$

which completes the proof. □

Lemma 6.31. *Let n, k, a, b, A, B as in Lemma 6.30.*

If

$$b^{\chi(k-1)} \cdot f_{k-1}\left(a, b^2\right) \neq 0 \ ,$$

then

$$B = \frac{b^{\chi(n-1)} \cdot f_{n-1}\left(a, b^2\right)}{b^{\chi(k-1)} \cdot f_{k-1}\left(a, b^2\right)}$$

and

$$A = a^k (-1)^{k-1} \frac{b^{\chi(n-k-1)} \cdot f_{n-k-1}\left(a, b^2\right)}{b^{\chi(k-1)} \cdot f_{k-1}\left(a, b^2\right)} \ .$$

Proof. Since

$$b^{\chi(k-1)} \cdot f_{k-1}\left(a, b^2\right) \neq 0 \ ,$$

thus by Lemma 6.30, we can formulate

$$B = \frac{b^{\chi(n-1)} \cdot f_{n-1}\left(a, b^2\right)}{b^{\chi(k-1)} \cdot f_{k-1}\left(a, b^2\right)} \ ,$$

whence again by Lemma 6.30 we obtain

$$
\begin{aligned}
A = a \cdot \Bigg(& \frac{b^{\chi(k-1)} \cdot f_{k-1}\left(a, b^2\right)}{b^{\chi(k-1)} \cdot f_{k-1}\left(a, b^2\right)} b^{\chi(n-2)} \cdot f_{n-2}\left(a, b^2\right) \\
& - \frac{b^{\chi(n-1)} \cdot f_{n-1}\left(a, b^2\right)}{b^{\chi(k-1)} \cdot f_{k-1}\left(a, b^2\right)} \cdot b^{\chi(k-2)} \cdot f_{k-2}\left(a, b^2\right) \Bigg) \\
= a \Bigg(& \frac{b^{\chi(k-1} f_{k-1}\left(a, b^2\right) b^{\chi(n-2)} f_{n-2}\left(a, b^2\right)}{b^{\chi(k-1)} \cdot f_{k-1}\left(a, b^2\right)} \\
& - \frac{b^{\chi(n-1)} f_{n-1}\left(a, b^2\right) \cdot b^{\chi(k-2)} f_{k-2}\left(a, b^2\right)}{b^{\chi(k-1)} \cdot f_{k-1}\left(a, b^2\right)} \Bigg) \ .
\end{aligned} \tag{6.12}
$$

By the definition of f_n, we have

$$
\begin{aligned}
b^{\chi(n)} f_n\left(a, b^2\right) &= b^{\chi(n)} (b^2)^{\left[\frac{n}{2}\right]} F_n\left(\frac{a}{b^2}\right) \\
&= b^{\chi(n)+2\left[\frac{n}{2}\right]} F_n\left(\frac{a}{b^2}\right) \\
&= b^n F_n\left(\frac{a}{b^2}\right) \ .
\end{aligned}
$$

Hence

$$
\begin{aligned}
& b^{\chi(k-1)} f_{k-1}\left(a, b^2\right) b^{\chi(n-2)} f_{n-2}\left(a, b^2\right) \\
& \qquad - b^{\chi(n-1)} f_{n-1}\left(a, b^2\right) \cdot b^{\chi(k-2)} f_{k-2}\left(a, b^2\right) \\
& = b^{k-1} F_{k-1}\left(\frac{a}{b^2}\right) b^{n-2} F_{n-2}\left(\frac{a}{b^2}\right) \\
& \qquad - b^{n-1} F_{n-1}\left(\frac{a}{b^2}\right) \cdot b^{k-2} F_{k-2}\left(\frac{a}{b^2}\right) \\
& = b^{n+k-3} \left(F_{k-1}\left(\frac{a}{b^2}\right) F_{n-2}\left(\frac{a}{b^2}\right) - F_{n-1}\left(\frac{a}{b^2}\right) \cdot F_{k-2}\left(\frac{a}{b^2}\right) \right) \ .
\end{aligned} \tag{6.13}
$$

By Lemma 6.1,

$$
F_{k-1}\left(\frac{a}{b^2}\right) F_{n-2}\left(\frac{a}{b^2}\right) - F_{n-1}\left(\frac{a}{b^2}\right) \cdot F_{k-2}\left(\frac{a}{b^2}\right) = (-1)^{k-1} \left(\frac{a}{b^2}\right)^{k-1} F_{n-k-1}\left(\frac{a}{b^2}\right) \ ,
$$

whence by (6.13), we have

$$
\begin{aligned}
& b^{\chi(k-1)} f_{k-1}\left(a, b^2\right) b^{\chi(n-2)} f_{n-2}\left(a, b^2\right) \\
& \qquad - b^{\chi(n-1)} f_{n-1}\left(a, b^2\right) \cdot b^{\chi(k-2)} f_{k-2}\left(a, b^2\right) \\
& = (-1)^{k-1} a^{k-1} b^{\chi(n-k-1)} f_{n-k-1}\left(a, b^2\right) \ .
\end{aligned}
$$

Substituting this into (6.12), we obtain

$$
A = a^k (-1)^{k-1} \frac{b^{\chi(n-k-1)} \cdot f_{n-k-1}\left(a, b^2\right)}{b^{\chi(k-1)} \cdot f_{k-1}\left(a, b^2\right)} \ . \quad \square
$$

Lemma 6.32. *Let $k, n \in \mathbb{N}$ and $A \in \mathbb{Z} \setminus \{0\}$ be fixed. Then there exist only finitely many, effectively computable $a, b, B \in \mathbb{Z}$, such that*

$$x^2 - bx - a \mid x^n - Bx^k - A \ .$$

Proof. First, let us determine $a, b \in \mathbb{Z}$, such that

$$\begin{gathered} b^{\chi(k-1)} \cdot f_{k-1}\left(a, b^2\right) \neq 0 \\ \text{and} \\ x^2 - bx - a \mid x^n - Bx^k - A \ . \end{gathered} \tag{6.14}$$

With these conditions, by Lemma 6.30, $a \mid A$, whence a may assume only finitely many different values and thus we may suppose that a is fixed.

Further, by Lemma 6.30,

$$0 = A \cdot b^{\chi(k-1)} \cdot f_{k-1}\left(a, b^2\right) - a^k(-1)^{k-1} b^{\chi(n-k-1)} \cdot f_{n-k-1}\left(a, b^2\right) \ , \tag{6.15}$$

which is an algebraic equation with indeterminate b and with finitely many solutions. The integer solutions of (6.15) are effectively computable, thus there exist only finitely many (effectively computable) pairs of a, b satisfying (6.14).

Since

$$f_{k-1}\left(a, b^2\right) \neq 0 \ ,$$

by Lemma 6.30, B is explicitly determinable from a and b, thus the set of the suitable B's is also finite and the values of B are effectively computable.

Now, assume that a, b are such that

$$b^{\chi(k-1)} f_{k-1}\left(a, b^2\right) = 0 \ . \tag{6.16}$$

Remark that $k > 1$, otherwise (6.16) would be equal to 1. We exclude the case $a = 0$, because by Lemma 6.30 we may write

$$A = a \cdot \left(b^{\chi(n-2)} \cdot f_{n-2}\left(a, b^2\right) - B \cdot b^{\chi(k-2)} \cdot f_{k-2}\left(a, b^2\right)\right) \ , \tag{6.17}$$

and thus $A = 0$ would hold.

Claim that

$$b^{\chi(k-2)} \cdot f_{k-2}\left(a, b^2\right) \neq 0 \ .$$

To prove, suppose the opposite.

First, let k be even. Then (6.16) looks like

$$b f_{k-1}\left(a, b^2\right) = 0 \ ,$$

whence either

$$b = 0$$

or

$$f_{k-1}\left(a, b^2\right) = 0$$

and

$$b^{\chi(k-2)} \cdot f_{k-2}\left(a, b^2\right) = f_{k-2}\left(a, b^2\right) \ .$$

If $k = 2$, then

$$f_{k-2}\left(a, b^2\right) = 1$$

or else if $k > 2$, then by definition, $f_{k-2}(x, y)$ is homogeneous, whence, if

$$b = 0 \quad \text{and} \quad f_{k-2}\left(a, b^2\right) = 0 \ ,$$

then $a = 0$, which was excluded.

Now, let k be odd. Then (6.16) has the form

$$f_{k-1}\left(a, b^2\right) = 0 \ ,$$

and

$$b^{\chi(k-2)} \cdot f_{k-2}\left(a, b^2\right) = b f_{k-2}\left(a, b^2\right) \ .$$

Since $f_{k-1}(x, y)$ is homogeneous, thus

$$b = 0 \quad \text{and} \quad f_{k-1}\left(a, b^2\right) = 0$$

yields that $a = 0$, which is, again, excluded.

If

$$f_{k-1}\left(a, b^2\right) = f_{k-2}\left(a, b^2\right) = 0 \ ,$$

then by Lemma 6.5,

$$f_l\left(a, b^2\right) = 0 \quad \text{for every} \quad l \geq k - 2 \ ,$$

in particular, for $l = n - 2$, whence by (6.17), $A = 0$, which is a contradiction. Thus our claim is proven.

By (6.17), $a \mid A$, thus a may have only finitely many different values. Furthermore, by (6.16), either

$$b = 0$$

or

$$b^{\chi(k-1)} f_{k-1}\left(a, b^2\right) = b^{k-1} F_{k-1}\left(\frac{a}{b^2}\right) = 0 \ ,$$

whence by Lemma 6.18,

$$\frac{a}{b^2} \in \left\{-1, -\frac{1}{2}, -\frac{1}{3}\right\} \ .$$

Hence, there exist only finitely many effectively computable a, b pairs satisfying equation (6.15).

Fix now a and b. Since

$$b^{\chi(k-2)} \cdot f_{k-2}\left(a, b^2\right) \neq 0 \ ,$$

thus (6.17) is a linear equation in B which has only one solution and this solution is explicitly given. Thus, we have found that a, b and B can have only finitely many values satisfying the conditions of the lemma in both cases and they are effectively computable. □

Lemma 6.33. *Let $k, n \in \mathbb{N}$, such that*

$$\gcd(n, k, 12) = 1$$

and $a, b, A, B \in \mathbb{Z}$, such that $A \cdot B \neq 0$.

If

$$x^2 - bx - a \mid x^n - Bx^k - A \ ,$$

then

$$b^{\chi(k-1)} f_{k-1}(a, b^2) \neq 0 \ .$$

Proof. To the contrary, suppose that

$$b^{\chi(k-1)} f_{k-1}(a, b^2) = 0 \ . \tag{6.18}$$

Then by Lemma 6.30,

$$b^{\chi(n-1)} f_{n-1}(a, b^2) = 0 \ ,$$

whence either

$$b^{\chi(n-1)} = 0$$

or

$$f_{n-1}(a, b^2) = 0 \ .$$

If

$$b^{\chi(n-1)} = 0 \ ,$$

then $b = 0$ and n is even.

Since

$$\gcd(n, k, 12) = 1 \ ,$$

thus k should be odd, whence

$$b^{\chi(k-1)} \neq 0$$

and by (6.18), we have

$$f_{k-1}(a, b^2) = 0 \ .$$

However, by the definition of f_{k-1}, the vanishing of $f_{k-1}(a, 0)$ implies that $a = 0$ and accordingly $A = 0$, which is a contradiction.

If

$$b^{\chi(n-1)} \neq 0 \ ,$$

then

$$f_{n-1}(a, b^2) = 0 \ ,$$

whence by similar considerations as above, $b \neq 0$.
Therefore, $\frac{a}{b^2}$ is a root of $F_{n-1}(x)$ and by (6.18) $\frac{a}{b^2}$ is a root of $F_{k-1}(x)$, too.
Hence, by Lemma 6.6, $\frac{a}{b^2}$ is a root of $F_{m-1}(x)$, where $m = \gcd(n, k)$.
Thus by Lemma 6.18,

$$\gcd(m, 12) \geq 3$$

and consequently,

$$\gcd(n, k, 12) \geq 3$$

which is a contradiction again. □

Theorem 6.34. *Let $k \in \mathbb{N}$, $A \in \mathbb{Z} \setminus \{0\}$. Then there exist only finitely many effectively computable polynomials in the form $x^n - Bx^k - A$, where $n \in \mathbb{N}$, such that $\gcd(n, k, 12) = 1$, $B \in \mathbb{Z} \setminus \{0\}$ and*

$$x^2 - bx - a \mid x^n - Bx^k - A$$

for some $a, b \in \mathbb{Z}$, supposing that either $a \neq -1$ or $|b| \neq 1$.

Proof. Suppose that $n \in \mathbb{N}$, such that $\gcd(n, k, 12) = 1$, $B \in \mathbb{Z} \setminus \{0\}$ and $a, b \in \mathbb{Z}$, such that $a \cdot |b| \neq -1$ and

$$x^2 - bx - a \mid x^n - Bx^k - A \ .$$

First, we prove that n is bounded.

By Lemma 6.33 and Lemma 6.31 we have

$$a^k(-1)^k \frac{b^{\chi(n-k-1)} \cdot f_{n-k-1}\left(a, b^2\right)}{b^{\chi(k-1)} \cdot f_{k-1}\left(a, b^2\right)} = A \ . \tag{6.19}$$

Since $A \neq 0$, thus $a \neq 0$, too. By the values of a and b we will distinguish different cases:

(i) Assume that $b^2 \geq 4|a|$. Then $|b| \geq 2$ and

$$\left|\frac{a}{b^2}\right| \leq \frac{1}{4} \ .$$

Hence, by Remark 6.21 and Remark 6.15,

$$\begin{aligned} \left|b^{\chi(k-1)} \cdot f_{k-1}\left(a, b^2\right)\right| &= \left|b^{k-1} F_{k-1}\left(\frac{a}{b^2}\right)\right| \\ &= \left|b^{k-1}\right| \cdot \left|F_{k-1}\left(\frac{a}{b^2}\right)\right| \\ &\leq |b|^{k-1} \cdot F_{k-1}\left(\frac{1}{4}\right) \end{aligned}$$

and

$$\begin{aligned} \left|b^{\chi(n-k-1)} \cdot f_{n-k-1}\left(a, b^2\right)\right| &= \left|b^{n-k-1} F_{n-k-1}\left(\frac{a}{b^2}\right)\right| \\ &= \left|b^{n-k-1}\right| \cdot \left|F_{n-k-1}\left(\frac{a}{b^2}\right)\right| \\ &\geq |b|^{n-k-1} \cdot F_{n-k-1}\left(-\frac{1}{4}\right) \ . \end{aligned}$$

Hence, by (6.19) and Remark 6.17, we obtain

$$\begin{aligned}
|A| &\geq \left| \frac{b^{\chi(n-k-1)} \cdot f_{n-k-1}\left(a, b^2\right)}{b^{\chi(k-1)} \cdot f_{k-1}\left(a, b^2\right)} \right| \\
&\geq \frac{|b|^{n-k-1} F_{n-k-1}\left(-\frac{1}{4}\right)}{|b|^{k-1} F_{k-1}\left(\frac{1}{4}\right)} \\
&= |b|^{n-2k} \frac{F_{n-k-1}\left(-\frac{1}{4}\right)}{F_{k-1}\left(\frac{1}{4}\right)} \\
&= |b|^{n-2k} \frac{(n-k-1)\left(\frac{1}{2}\right)^{n-k-1}}{F_{k-1}\left(\frac{1}{4}\right)} \\
&= (n-k-1)\left(\frac{|b|}{2}\right)^{n-2k} \frac{1}{2^{k-1} F_{k-1}\left(\frac{1}{4}\right)} \quad ,
\end{aligned}$$

i.e.

$$2^{k-1} F_{k-1}\left(\frac{1}{4}\right) |A| \geq (n-k-1)\left(\frac{|b|}{2}\right)^{n-2k} \quad .$$

Since $|b| \geq 2$, the above yields that n is bounded. A rough upper bound:

$$n \leq \max\left\{ 2k, 2^{k-1} F_{k-1}\left(\frac{1}{4}\right) |A| + k + 1 \right\} \quad .$$

(ii) Consider now the case $0 \neq b^2 < 4a \leq 4|A|$.
Then, by Remark 6.15 and Remark 6.17,

$$\begin{aligned}
|A| &\geq \left| \frac{b^{\chi(n-k-1)} \cdot f_{n-k-1}\left(a, b^2\right)}{b^{\chi(k-1)} \cdot f_{k-1}\left(a, b^2\right)} \right| \\
&\geq \frac{|b|^{n-k-1} F_{n-k-1}\left(\frac{1}{4}\right)}{|b|^{k-1} F_{k-1}\left(\frac{a}{b^2}\right)} \\
&= |b|^{n-2k} \frac{\frac{2+\sqrt{2}}{4}\left(\frac{1+\sqrt{2}}{2}\right)^{n-k-1} + \frac{2-\sqrt{2}}{4}\left(\frac{1-\sqrt{2}}{2}\right)^{n-k-1}}{F_{k-1}\left(\frac{a}{b^2}\right)} \\
&\geq |b|^{n-2k} \frac{\frac{1}{2}\left(\frac{1+\sqrt{2}}{2}\right)^{n-k-1} - 1}{F_{k-1}\left(\frac{a}{b^2}\right)} \\
&\geq |b|^{n-2k} \frac{\frac{1}{2}\left(\frac{1+\sqrt{2}}{2}\right)^{n-k-1} - 1}{F_{k-1}\left(|A|\right)} \quad ,
\end{aligned}$$

whence

$$2|A| \cdot F_{k-1}\left(|A|\right) \geq |b|^{n-2k} \left(\left(\frac{1+\sqrt{2}}{2}\right)^{n-k-1} - 2 \right)$$

and thus n is bounded. An upper bound is

$$n \leq \max\left\{2k, \frac{\log\left(2|A| \cdot F_{k-1}\left(|A|\right)\right)}{\log\left(\frac{1+\sqrt{2}}{2}\right)} + k + 1\right\} \ .$$

(iii) Further, we proceed with the case $0 \neq b^2 < -4a \leq 4|A|$.
Clearly, $a \neq -1$, otherwise $0 \neq b^2 < -4a = 4$ would imply that $|b| = 1$, which would contradict $a \cdot |b| \neq -1$. By Lemma 6.29, if

$$n > \widehat{c}_1 = \max_{a|A,\ b^2 \leq -4a} \left\{c_1(a, b^2)\right\} \ ,$$

where c_1 defined in the lemma, we get

$$f_n\left(a, b^2\right) > 2^{\frac{n}{4}} \ .$$

Let

$$\widehat{f} = \max_{a|A,\ b^2 \leq -4a} \left\{|b^{\chi(k-1)} \cdot f_{k-1}(a, b^2)|\right\} \ .$$

We know that $\widehat{f} > 0$. If $n > \widehat{c}_1 + k + 1$, then

$$|A| \geq \left|\frac{b^{\chi(n-k-1)} \cdot f_{n-k-1}\left(a, b^2\right)}{b^{\chi(k-1)} \cdot f_{k-1}\left(a, b^2\right)}\right| \geq \frac{2^{\frac{n-k-1}{4}}}{\widehat{f}} \ .$$

Thus n is bounded. A rough estimate

$$n \leq \max\left\{(\widehat{c}_1 + k + 1, 4\log_2\left(|A|\widehat{f}\right) + k + 1\right\} \ .$$

(iv) Finally, if $b = 0$, then by Lemma 6.30, k and n should be even, otherwise $A = 0$. Nevertheless, $\gcd(n, k, 12) = 1$ which is a contradiction, thus the case $b = 0$ cannot occur.

Finally, we have found that in all the cases n is bounded and the upper bound depends only on k and A, whence by Lemma 6.32 the statement of the theorem follows. □

Theorem 6.35. *Let $n, k \in \mathbb{N}$, such that $\gcd(n, k, 12) = 1$ and $n - k > 4$ and let $B \in \mathbb{Z} \setminus \{0\}$ are fixed. Then there exist only finitely many $A \in \mathbb{Z} \setminus \{0\}$, such that*

$$x^2 - bx - a \mid x^n - Bx^k - A$$

for some $a, b \in \mathbb{Z}$.

Proof. Let $a, b, A \in \mathbb{Z}$, such that $A \neq 0$ and

$$x^2 - bx - a \mid x^n - Bx^k - A \ .$$

Then, by Lemma 6.33

$$b^{\chi(k-1)} \cdot f_{k-1}\left(a, b^2\right) \neq 0 \ ,$$

whence by Lemma 6.30

$$B \cdot b^{\chi(k-1)} \cdot f_{k-1}\left(a, b^2\right) = b^{\chi(n-1)} \cdot f_{n-1}\left(a, b^2\right) \tag{6.20}$$

and

$$A = a \cdot \left(b^{\chi(n-2)} \cdot f_{n-2}\left(a, b^2\right) - B \cdot b^{\chi(k-2)} \cdot f_{k-2}\left(a, b^2\right)\right) \ . \tag{6.21}$$

Hence by Lemma 6.22,

$$\begin{aligned} b^{\chi(k-1)} \cdot f_{k-1}\left(a, b^2\right) \cdot A &= a \cdot \Big(b^{\chi(k-1)} \cdot f_{k-1}\left(a, b^2\right) \cdot b^{\chi(n-2)} \cdot f_{n-2}\left(a, b^2\right) \\ &\quad - B \cdot b^{\chi(k-1)} \cdot f_{k-1}\left(a, b^2\right) \cdot b^{\chi(k-2)} \cdot f_{k-2}\left(a, b^2\right)\Big) \\ &= a \cdot \Big(b^{\chi(k-1)} \cdot f_{k-1}\left(a, b^2\right) \cdot b^{\chi(n-2)} \cdot f_{n-2}\left(a, b^2\right) \\ &\quad - b^{\chi(n-1)} \cdot f_{n-1}\left(a, b^2\right) \cdot b^{\chi(k-2)} \cdot f_{k-2}\left(a, b^2\right)\Big) \\ &= (-1)^{k-1} a^k b^{2k-1} b^{\chi(n-k-1)} \cdot f_{n-k-1}\left(a, b^2\right) \ , \end{aligned}$$

whence

$$b^{\chi(k-1)} \cdot f_{k-1}\left(a, b^2\right) \cdot A \neq 0$$

implies that $a \neq 0$ and $b \neq 0$.

By (6.20) and Remark 6.21, we have

$$B \cdot F_{k-1}\left(\frac{a}{b^2}\right) = b^{n-k} \cdot F_{n-1}\left(\frac{a}{b^2}\right) \ . \tag{6.22}$$

Since $\deg(F_{k-1}) = \left[\frac{k-1}{2}\right]$ and $\deg(F_{n-1}) = \left[\frac{n-1}{2}\right]$, thus there exist real numbers $M_1, M_2, x_1, x_2 > 0$, such that if $|x| > x_1$, then

$$|F_{k-1}(x)| < M_1 \cdot |x|^{\left[\frac{k-1}{2}\right]}$$

and if $|x| > x_2$, then

$$|F_{n-1}(x)| > M_2 \cdot |x|^{\left[\frac{n-1}{2}\right]}$$

with $M_1, M_2 > 0$.

Let $x_0 = \max(1, x_1, x_2)$ and suppose that $\left|\frac{a}{b^2}\right| > x_0$. Then

$$B \cdot M_1 \cdot \left|\frac{a}{b^2}\right|^{\left[\frac{k-1}{2}\right]} > B \cdot F_{k-1}\left(\frac{a}{b^2}\right) = \left|b^{n-k}\right| \cdot F_{n-1}\left(\frac{a}{b^2}\right) > \left|b^{n-k}\right| \cdot M_2 \cdot \left|\frac{a}{b^2}\right|^{\left[\frac{n-1}{2}\right]} \ .$$

Hence,

$$\frac{B \cdot M_1}{M_2} > \left|b^{n-k}\right| \cdot \left|\frac{a}{b^2}\right|^{\left[\frac{n-1}{2}\right]-\left[\frac{k-1}{2}\right]} > \left|b^{n-k}\right| \cdot (x_0)^{\left[\frac{n-1}{2}\right]-\left[\frac{k-1}{2}\right]} \ .$$

This yields that b is bounded, whence by (6.20) and (6.21) the integers a and A are also bounded.

Now suppose that $\left|\frac{a}{b^2}\right| \leq x_0$ and let

$$l = \frac{1}{2} \min \left\{ |x_i - x_j| \mid 0 < i, j \leq \left[\frac{n-1}{2}\right] \right\} ,$$

where $x_1 \dots x_{\left[\frac{n-1}{2}\right]}$ are the roots of the polynomial $F_{n-1}(x)$.

Then

$$\left| F_{k-1}\left(\frac{a}{b^2}\right) \right| \leq M$$

with some M and clearly, $l > 0$.

If

$$\min \left\{ \left| x_i - \frac{a}{b^2} \right| \mid 0 < i \leq \left[\frac{n-1}{2}\right] \right\} \geq l ,$$

then

$$\left| F_{n-1}\left(\frac{a}{b^2}\right) \right| = \prod_{i=1}^{\left[\frac{n-1}{2}\right]} \left| x_i - \frac{a}{b^2} \right| \geq l^{\left[\frac{n-1}{2}\right]} ,$$

whence by (6.22),

$$\frac{B \cdot M}{l^{\left[\frac{n-1}{2}\right]}} \geq \left| b^{n-k} \right|$$

and thus b is bounded. Since $|a| \leq x_0 \cdot b^2$, thus a is bounded, whence by (6.21) A is also bounded.

If

$$\min \left\{ \left| x_i - \frac{a}{b^2} \right| \mid 0 < i \leq \left[\frac{n-1}{2}\right] \right\} < l ,$$

then by the definition of l, there exists a unique $i_0 \in \{1, \dots, \left[\frac{n-1}{2}\right]\}$, such that $\left| x_{i_0} - \frac{a}{b^2} \right| < l$. With this i_0 we have

$$\left| F_{n-1}\left(\frac{a}{b^2}\right) \right| \geq l^{\left[\frac{n-3}{2}\right]} \cdot \left| x_{i_0} - \frac{a}{b^2} \right| ,$$

whence by (6.22) we get

$$\frac{B \cdot M}{l^{\left[\frac{n-3}{2}\right]} \cdot \left| b^{n-k} \right|} \geq \left| x_{i_0} - \frac{a}{b^2} \right| . \tag{6.23}$$

Since

$$b \cdot f_{n-1}\left(a, b^2\right) \neq 0 ,$$

thus

$$F_{n-1}\left(\frac{a}{b^2}\right) \neq 0 ,$$

whence $x_{i_0} \neq \frac{a}{b^2}$.

We assumed $n-k > 4$, whence the theorem of Roth on approximation of algebraic numbers [39] implies that there exist only finitely many suitable pairs of $a, b \in \mathbb{Z}$ satisfying (6.23) for every x_{i_0} root of $F_{n-1}(x)$. The number of the roots of $F_{n-1}(x)$ is finite, thus a and b are bounded, whence A can be chosen from a finite set. $\square$

Theorem 6.36. *Let $n, k \in \mathbb{N}$, such that $\gcd(n,k,12) \geq 2$ and $n-k>4$ and let $B \in \mathbb{Z} \setminus \{0\}$ are fixed. Then there exists an explicitly given sequence of integers A_i $(i=1,\dots)$, such that*

$$x^2 - bx - a \mid x^n - Bx^k - A_i \tag{6.24}$$

for some $a,b \in \mathbb{Z}$ and there are no other A's satisfying (6.24).

Proof. Let $\gcd(n,k,12) = m > 1$. Then by Lemma 6.23, there exist

$$g_1(x,y), g_2(x,y) \in \mathbb{Z}[x,y]$$

, such that

$$y^{\chi(n-1)} \cdot f_{n-1}\left(x,y^2\right) = g_1(x,y) \cdot y^{\chi(m-1)} \cdot f_{m-1}\left(x,y^2\right) \ ,$$

$$y^{\chi(k-1)} \cdot f_{k-1}\left(x,y^2\right) = g_2(x,y) \cdot y^{\chi(m-1)} \cdot f_{m-1}\left(x,y^2\right) \ .$$

Furthermore, by Lemma 6.30, we have

$$B \cdot g_2(x,y) \cdot y^{\chi(m-1)} \cdot f_{m-1}\left(x,y^2\right) = g_1(x,y) \cdot y^{\chi(m-1)} \cdot f_{m-1}\left(x,y^2\right) \ . \tag{6.25}$$

The a,b solutions of (6.25) are such that either

$$b^{\chi(m-1)} \cdot f_{m-1}\left(a,b^2\right) = 0 \tag{6.26}$$

or

$$b^{\chi(m-1)} \cdot f_{m-1}\left(a,b^2\right) \neq 0 \ . \tag{6.27}$$

If (6.26) holds, then either $b=0$ or $F_{m-1}\left(\frac{a}{b^2}\right) = 0$. If $b=0$, then $a \in \mathbb{Z}$ is arbitrary and by Lemma 6.30,

$$A = a \cdot \left(b^{\chi(n-2)} \cdot f_{n-2}\left(a,b^2\right) - B \cdot b^{\chi(k-2)} \cdot f_{k-2}\left(a,b^2\right)\right) \ .$$

If $F_{m-1}\left(\frac{a}{b^2}\right) = 0$, then by Lemma 6.18,

$$\frac{a}{b^2} \in \left\{-1, -\frac{1}{2}, -\frac{1}{3}\right\} \ ,$$

whence, again by Lemma 6.30, A can be explicitly determined.

If (6.27) holds, then we can cancel out $b^{\chi(m-1)} \cdot f_{m-1}\left(a,b^2\right)$ from (6.25) and the simplified equation can be solved in similar way as (6.20) in the proof of Theorem 6.35. □

Remark 6.37. *Schinzel showed that there exist a constant c such that every trinomial with integer coefficients having the property $n/\gcd(n,k) > c$ is reducible if and only if it has a linear or quadratic divisor. (See Consequence 1. of* [40].*) He also proved some results similar to our Theorems 6.34, 6.35 and 6.36 in Theorem 9 of* [40].

Appendix A

A linear recurring sequence having uniform distribution

In this appendix we give an example of a 1281^{st} order linear recurring sequence which is uniformly distributed modulo 2^n for any n. The sequence is created by the method given in Construction 4.22.

The coefficients of the recurrence relation are the following:

3, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0,
0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0,
0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1,
0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0,
0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1,
0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1,
1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0,
0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1,
0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1,
0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1,
1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0,
0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1,
0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1,
0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1,
0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1,
0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1,
1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1,
0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1,
0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0,
1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0,
1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0,
0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1,
0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0,
0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0,
0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0,
0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1,
0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1,
1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1 .

The corresponding recurrence relation:

$$u_n = u_{n-1} + u_{n-3} + \cdots + u_{n-1279} + u_{n-1280} + 3u_{n-1281} \ .$$

A possible set of initial values $u_0 = u_1 = \cdots = u_{1279} = 0$, $u_{1280} = 1$. Another, "more random" initial values:

996, 302, 830, 19, 782, 386, 997, 207, 158, 592, 757, 948, 774, 577, 592, 528, 25, 481, 30, 873, 491, 231, 288, 263, 16, 362, 313, 360, 53, 220, 705, 374, 689, 444, 999, 152, 434, 982, 966, 119, 449, 957, 631, 854, 422, 720, 159, 36, 241, 46, 436, 15, 855, 726, 860, 489, 437, 174, 775, 12, 5, 392, 34, 602, 483, 887, 14, 293, 128, 583, 727, 612, 779, 749, 361, 980, 391, 609, 143, 507, 21, 549, 426, 113, 701, 372, 459, 910, 935, 36, 416, 462, 815, 613, 817, 113, 917, 275, 313, 704, 155, 818, 902, 85, 887, 467, 200, 47, 128, 147, 341, 598, 450, 778, 51, 527, 241, 1015, 1017, 114, 761, 579, 92, 536, 503, 1011, 813, 200, 226, 113, 702, 423, 900, 420, 162, 922, 600, 11, 153, 50, 304, 881, 894, 338, 534, 842, 680, 822, 341, 672, 225, 762, 527, 655, 176, 86, 932, 272, 711, 279, 147, 416, 667, 791, 976, 224, 642, 55, 891, 60, 560, 616, 899, 59, 706, 60, 308, 391, 322, 667, 942, 406, 697, 207, 241, 41, 872, 54, 1014, 124, 878, 649, 765, 288, 884, 981, 951, 457, 1010, 186, 165, 199, 441, 688, 607, 215, 749, 130, 637, 219, 606, 922, 168, 85, 734, 342, 663, 343, 679, 259, 843, 392, 727, 521, 693, 812, 206, 673, 312, 898, 664, 355, 486, 205, 391, 543, 736, 826, 196, 599, 539, 748, 522, 17, 791, 196, 923, 973, 90, 728, 720, 768, 585, 858, 150, 234, 485, 894, 280, 201, 151, 611, 142, 682, 992, 302, 377, 226, 790, 726, 144, 435, 780, 747, 333, 379, 64, 226, 333, 680, 440, 108, 567, 751, 418, 213, 31, 575, 139, 171, 369, 508, 585, 22, 523, 970, 476, 858, 2, 597, 62, 569, 413, 614, 200, 505, 292, 70, 201, 654, 433, 291, 170, 564, 750, 1017, 776, 131, 203, 270, 756, 519, 860, 606, 606, 478, 131, 798, 742, 525, 1003, 833, 219, 130, 372, 715, 219, 186, 755, 751, 424, 712, 702, 686, 288, 592, 542, 585, 8, 556, 117, 7, 1019, 622, 561, 419, 777, 781, 944, 174, 788, 942, 422, 705, 847, 245, 98, 772, 609, 108, 230, 524, 446, 197, 921, 337, 246, 878, 660, 613, 709, 614, 221, 170, 768, 385, 868, 431, 206, 719, 183, 833, 860, 705, 939, 574, 534, 762, 209, 481, 738, 490, 416, 658, 521, 308, 272, 926, 774, 446, 114, 396, 716, 794, 990, 35, 900, 708, 724, 777, 893, 774, 129, 633, 494, 95, 287, 17, 783, 860, 768, 110, 345, 293, 359, 289, 919, 451, 77, 304, 618, 655, 567, 903, 475, 226, 131, 157, 752, 291, 327, 147, 871, 501, 17, 447, 860, 876, 63, 609, 223, 604, 576, 41, 260, 164, 495, 12, 744, 544, 711, 125, 138, 514, 647, 829, 149, 796, 193, 309, 9, 302, 103, 884, 771, 276, 879, 856, 108, 775, 373, 760, 183, 537, 4, 932, 881, 563, 802, 683, 77, 31, 537, 781, 967, 226, 1007, 532, 36, 931, 72, 608, 193, 753, 404, 220, 56, 703, 559, 994, 710, 771, 89, 142, 62, 594, 713, 465, 908, 86, 736, 848, 399, 1016, 168, 154, 970, 693, 59, 31, 873, 753, 898, 51, 1019, 134, 792, 747, 288, 212, 94, 613, 442, 824, 223, 524, 941, 528, 6, 805, 548, 58, 17, 72, 801, 817, 768, 0, 942, 421, 640, 374, 934, 361, 845, 748, 379, 878, 905, 966, 997, 878, 922, 238, 163, 587, 145, 383, 743, 459, 226, 919, 29, 212, 873, 183, 11, 776, 755, 917, 291, 505, 601, 760, 728, 185, 298, 837, 467, 600, 26, 335, 751, 871, 493, 642, 905, 436, 303, 503, 156, 52, 118, 508, 706, 1011, 209, 150, 720, 27, 420, 80, 207, 930, 576, 335, 344, 348, 904, 492, 445, 642, 644, 162, 932, 545, 899, 740, 977, 260, 976, 745, 846, 520, 625, 276, 853, 769, 843, 884, 820, 624, 868, 566, 1022, 453, 371, 290, 128, 94, 659, 435, 162, 633, 195, 1017, 988, 735, 16, 542, 90, 646, 54, 839, 45, 726, 299, 515, 618, 225, 572, 826, 181, 340, 1017, 390, 21, 302, 90, 649, 527, 766, 90, 412, 515, 512, 339, 203, 656, 703, 157, 591, 987, 891, 355, 846, 340, 202, 339, 11, 10, 544, 138, 773, 544, 821, 246, 593, 528, 579, 114, 907, 439, 821, 301, 17, 623, 475, 845, 727, 901, 246, 797, 358, 37, 672, 322, 505, 622, 503, 476, 799, 626, 996, 756, 609, 887, 497, 454, 444, 142, 639, 899, 388, 591, 424, 502, 379, 104, 548, 235, 635, 705, 232, 874, 847, 929, 893, 195, 272, 623, 50, 681, 154, 540, 840, 606, 676, 488, 531, 151, 822, 693, 65, 318, 973, 85, 96, 43, 440, 821, 173, 156, 252, 522, 107, 916, 583, 312, 304, 97, 280, 568, 272, 120, 1000, 100, 368, 1009, 811, 782, 823, 884, 842, 810, 847, 665, 305, 165, 128, 935, 453, 365, 156, 833, 697, 740, 982, 660, 750, 187, 194, 675, 267, 396, 547, 236, 855, 917, 975, 330, 600, 686, 590, 932, 68, 620, 742, 184, 602, 68, 687, 353, 761, 1002, 639, 488, 387, 941, 383, 612, 874, 101, 28, 359, 472, 1023, 903, 646, 73, 804, 894, 491, 643, 699, 27, 437, 965, 987, 239, 564, 361, 815, 670, 141, 797, 783, 41, 806, 670, 578, 307, 869, 82, 413, 14, 174, 666, 658, 60, 864, 948, 423, 1005, 140, 469, 395, 196, 583, 220, 756, 1, 921, 519, 425, 777, 296, 731, 852, 190, 615, 209, 505, 873, 213, 676, 821, 403, 624, 449, 415, 218, 866, 412, 376, 256, 1011, 908, 567, 997, 12, 884, 171, 888, 918, 382, 450, 943, 216, 436, 882, 296, 354, 331, 313, 469, 513, 955, 759, 315, 252, 173, 101, 535, 404, 733, 162, 107, 810, 825, 665, 684, 475, 766, 489, 739, 573, 823, 822, 648, 713, 412, 302, 981, 111, 520, 420, 39, 553, 797, 333, 645, 787, 929, 337, 79, 929, 893, 62, 1, 354, 566, 473, 242, 262, 925, 578, 3, 472, 621, 45, 372, 416, 769, 641, 703, 44, 265, 1004, 430, 127, 34, 571, 377, 135, 37, 944, 559, 733, 758, 660, 143, 265, 108, 985, 752, 13, 926, 535, 175, 566, 519, 455, 106, 47, 302, 678, 536, 794, 475, 321, 208, 260, 4, 875, 211, 324, 145, 535, 167, 147, 998, 213, 260, 469, 895, 731, 873, 267, 872, 702, 154, 101, 915, 328, 703, 82, 469, 543, 325, 448, 761, 518, 49, 895, 665, 117, 995, 726, 102, 179, 615, 17, 1022, 946, 973, 582, 491, 941, 126, 539, 860, 462, 359, 6, 925, 544, 880, 721, 818, 528, 163, 381, 426, 606, 109, 271, 515, 986, 569, 528, 989, 823, 6, 920, 966, 450, 398, 12, 793, 895, 636, 442, 390, 437, 530, 159, 981, 282, 286, 154, 404, 532, 943, 850, 928, 703, 595, 140, 218, 95, 884, 259, 824, 845, 383, 233, 6, 434, 76, 320, 884, 189, 639, 178, 82, 142, 855, 169, 810, 882, 604, 110, 257, 298, 419, 389, 518, 815, 491, 268, 781, 838, 54, 439, 505, 453, 196, 374, 846, 344, 916, 758, 391, 921, 66, 1014, 293, 703, 56, 677, 577, 454, 104, 595, 86, 421, 125, 969, 92, 748, 763, 396, 746, 18, 564, 178, 912, 932, 821, 979, 906, 606, 838, 714, 823, 845, 379, 714, 988, 568, 865, 610, 133, 240, 85, 151, 350, 614, 645, 595, 609, 434, 446, 808, 326, 740, 706, 136, 843, 709, 111, 613, 320, 875, 904, 297, 509, 807, 824, 49, 666, 733, 1001, 783, 384, 221, 121, 688, 257, 19,

where $u_0 = 996$, $u_1 = 302$, $u_2 = 830$, ...

Appendix B

Experiments with transformation of uniformly distributed sequences

Some computational experiments have been made concerning the construction of Gaussian distributed random number generation of Chapter 5. We have created some random number generators and tested them by linear transformations. For computations we used the Maple package. The programs are available by the authors.

Figure 1. This is the graph of the density (relative frequency) function of the transformed Fibonacci sequence modulo 5. The used linear transformation: $x_n = (\hat{F}_{n+1} + \hat{F}_n - 2)/4$, where

a.) $\hat{F}_n$ is the nth Fibonacci number reduced modulo 5.
b.) $\hat{F}_n$ is the nth Fibonacci number reduced modulo 125.
c.) $\hat{F}_n$ is the nth Fibonacci number reduced modulo 3125.
c.) $\hat{F}_n$ is the nth Fibonacci number reduced modulo 78125.

Figure 2. This is the graph of the density (relative frequency) function of the transformed sequence of u_n, where

$$u_{n+9} = u_{n+8} + u_{n+3} + 2u_{n+1} + u_n$$

is the impulse response sequence. The used linear transformation at figures

a.) b.) c.) and d.) are the summation of the four consecutive elements of the sequence with proper constant weight multiplier

e.) f.) g.) and h.) are the summation of the six consecutive elements of the sequence with proper constant weight multiplier

i.) j.) k.) and l.) are the summation of the eight consecutive elements of the sequence with proper constant weight multiplier.

The sequences are reduced at figures

a.) e.) and i.) modulo 2
b.) f.) and j.) modulo 16
c.) g.) and k.) modulo 1024
d.) h.) and l.) modulo 65536.

Figure 3. This is the graph of the density (relative frequency) function of the transformed sequence of u_n, where

$$\begin{aligned} u_{n+33} = {} & u_{n+31} + u_{n+29} + u_{n+26} + u_{n+25} + u_{n+23} + u_{n+22} + u_{n+21} \\ & + u_{n+20} + u_{n+19} + u_{n+17} + u_{n+16} + u_{n+14} + u_{n+13} + u_{n+12} \\ & + u_{n+10} + u_{n+8} + u_{n+4} + u_{n+1} + u_n \end{aligned}$$

is the impulse response sequence. The used linear transformation at figures

a.) b.) c.) and d.) are the summation of the 10 consecutive elements of the sequence with proper constant weight multiplier

e.) f.) g.) and h.) are the summation of the 20 consecutive elements of the sequence with proper constant weight multiplier

i.) j.) k.) and l.) are the summation of the 35 consecutive elements of the sequence with proper constant weight multiplier.

The sequences are reduced at figures

a.) e.) and i.) modulo 2

b.) f.) and j.) modulo 16

c.) g.) and k.) modulo 1024

d.) h.) and l.) modulo 65536.

References

1. R. N. Bhattacharya and R. Ranga Rao, *Normal Approximation and Asymptotic Expansions*, Wiley series in probability and mathematical statistics, John Wiley & Sons, Inc., New York, London, Sydney, Toronto, 1976.
2. T.S. Blyth, *Module Theory*, Oxford University Press, 1977.
3. R.T. Bumby, *A distribution property for linear recurrence of the second-order*, Proc. Amer. Math. Soc. **50** (1975), 101–106.
4. P. Bundschuh, *On the distribution of Fibonacci numbers*, Tamkang J. **5** (1974), 75–79.
5. P. Bundschuh, J. Shiue, *Solution of a problem on the uniform distribution of integers*, Atti Accad. Naz. Lincei, Rend. Cl. Sci. fis. mat. nat. **55** (1973), 172–177.
6. W. Carlip, E. Jacobson, *A criterion for stability of two-term recurrence sequences modulo* 2^k, Finite Fields and Their Appl. **2** (1996), 369–406.
7. P. M. Cohn, *Algebra*, John Wiley & Sons, Chichester, New York, Brisbane, Toronto, 1979.
8. L. Devroye, *Nonuniform Random Variate Generation*, Springer-Verlag, New York Berlin, 1986.
9. E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial*, Acta Arith. **34** (1979), 391–401.
10. M. Drmota, R.F. Tichy, *Sequences, Discrepancies and Applications*, vol. 1651, Lecture Notes in Mathematics, Springer-Verlag, 1997.
11. M. Drmota and R.F. Tichy, *C-Uniform Distribution on Compact Metric Spaces*, Journal of Math. Anal. and Appl. **123 No 1** (1988).
12. M. Drmota, R.F. Tichy and R. Winkler, *Completely uniform distributed sequences of matrices*, Number-Theoretic Analysis (E. Hlawka and R.F. Tichy, eds.), Vienna 1988-89, vol. **1452**, Springer-Verlag, Berlin Heidelberg New York London Paris Tokyo Hong Kong Barcelona, 1990, pp. 43-57.
13. H.J.A. Duparc, *Periodicity properties of recurring sequences. I*, Nederl. Akad. Wet., Proc. **Ser. A 57** (1954), 331–342.
14. H.J.A. Duparc, *Periodicity properties of recurring sequences. II*, Nederl. Akad. Wet., Proc. **Ser. A 58** (1955), 472–485.
15. E. Fried, *Általános algebra*, Tankönyvkiadó, Budapest, 1981.
16. L. Fuchs, *Algebra*, Tankönyvkiadó, Budapest, 1970.
17. M. Goldstern, *Eine Klasse Vollständig Gleichverteiler Folgen*, Lecture Notes in Mathematics **1262** (1987), Springer-Verlag, Berlin Heidelberg New York London Paris Tokyo, 37-45.
18. T. Herendi, *On an Optical Character Recognition Method*, 2nd Conference On Artifical Intelligence, vol. 2, Budapest, 1991, pp. 373-380.
19. T. Herendi, *Uniform distribution of linear recurring sequences modulo prime powers*, Finite Fields and Applications (to appear).
20. T. Herendi, T. Siegl, R.F. Tichy, *A Note on Non-Uniformly Distributed Pseudorandom Number Generation Using Linear Transformations*, Computing **59** (1997), 163-181.
21. T. Herendi, A. Pethő, *Trinomials Which are Divisible by Quadratic Polynomials*, Acta Ac. Paed. Agriensis (1994), 61-73.
22. D. E. Knuth, *The Art of Computer Programming*, vol. 3, Addison-Wesley, 1973.
23. L. Kuipers and H. Niederreiter, *Uniform distribution of sequences*, John Wiley & Sons, New York London Sydney Toronto, 1974.
24. R. Lidl, H. Niederreiter, *Introduction to finite fields and their applications*, Cambridge University Press, 1986.

25. T. Nagell, *Sur la réductibilité des trinômes*, Comptes rendus du 8. congrès des mathématiciens scandinaves, Stockholm (1934), 273–275.
26. W. Narkiewicz, *Number Theory*, World Scientific Publishing Co. Pte. Ltd., Singapore, 1977.
27. W. Narkiewicz, *Uniform Distribution of Sequences of Integers in Residue Classes*, vol. 1087, Lecture Notes in Mathematics, Springer-Verlag, 1984.
28. M.B. Nathanson, *Linear recurrences and uniform distribution*, Proc. Amer. Math. Soc. **48** (1975), no. 2, 289–291.
29. H. Niederreiter, *Distribution of Fibonacci numbers* mod 5^k, Fibonacci Quart. **10** (1972), no. 4, 373–374.
30. H. Niederreiter, *Pseud-orandom Number Generation and Quasi-Monte Carlo Methods*, Society for Industrial and Applied Mathematics, Philadelphia, Pennsylvania, 1992.
31. H. Niederreiter, J.S.Shiue, *Equidistribution of linear recurring sequences in finite fields*, Indag. Math. **39** (1977), 397–405.
32. H. Niederreiter, J.S.Shiue, *Equidistribution of linear recurring sequences in finite fields. II*, Acta Arith. **38** (1980), 197–207.
33. H. Niederreiter and J.M Wills, *Diskrepanz und Distanz von Maßen bezüglich konvexer und Jordanscher Mengen*, Math. Z. **144** (1975), 125-134.
34. A. Pethő, *Perfect Powers in Second Order Linear Recurrences*, J. of Number Theory **15** (1982), 5-13.
35. M. Pohst and H. Zassenhaus, *Algorithmic algebraic number theory*, Cambridge University Press, Cambridge, New York, Port Chester, Melbourne, Sydney, 1989.
36. G. Rauzy, *Discrepance d'une Suite Complement Equirepartie*, Annales Faculté des Sciences Toulouse **III** (1981), 105-112.
37. L. Rédei, *Lückenhafte Polynome über endlichen Körpern*, vol. 42, Lehrbücher und Monographien aus dem Gebiete der exakten Wissenschaften, Mathematische Reihe, Birkhäuser Verlag, Basel-Stuttgart, 1970.
38. P. Ribenboim, *On the factorization of* $x^n - B * x - A$, Enseign. - Math. **37** (1991), 191–200.
39. K. F. Roth, *Rational approximations to algebraic numbers*, Mathematika **2** (1955), 1–20.
40. A. Schinzel, *On reducible polynomials*, Dissertationes Mathematicae **329** (1993).
41. A. Schinzel, *On reducible polynomials II.*, Publicationes Mathematicae **56, No. 3–4** (2000), 575–608.
42. A. Schinzel, *On reducible polynomials III.*, Periodica Mathematica Hungarica **43, No. 1–2** (2001), 43–69.
43. T.N. Shorey, R. Tijdeman, *Exponential Diophantine Equations*, Cambridge University Press, Cambridge Tracts in Mathematics, 87., 1986.
44. R.F. Tichy, *Contributions to General Algebra 5, Proceedings of the Salzburg Conference, Mai 29- June 1, 1986*, Verlag Hoelder-Pichler-Tempsky, Wien 1987 - Verlag B.G. Teubner, Stuttgart, pp. 401–406.
45. R.F. Tichy, G. Turnwald, *Uniform distribution of recurrences in Dedekind domains*, Acta Arith. (1985), 81–89.
46. G. Turnwald, *Uniform distribution of second-order linear recurring sequences*, Proc. Amer. Math. Soc. **96** (1986), no. 2, 189–198.
47. G. Turnwald, *Gleichverteilung von linearen rekursiven Folgen*, Sitzungber., Abt. II, Oesterr. Akad. Wiss., Math.-Naturwiss. **193** (1985), 201–245.
48. B. L. van der Waerden, *Algebra*, Frederick Ungar Publishing Co., New York, 1970.
49. M. Ward, *The characteristic number of a sequence of integers, satisfying a linear recursion relation*, Trans. Amer. Math. Soc. **33** (1931), 153–165.
50. M. Ward, *The distribution of residues in sequences satisfying a linear recurrence relation*, Trans. Amer. Math. Soc. **33** (1931), 166–190.
51. W.A. Webb, C.T. Long, *Distribution modulo* p^k *of the general linear second-order recurrence*, Atti Accad. Naz. Lincei, Rend. Cl. Sci. fis. mat. nat **58** (1975), 92–100.
52. R. Winkler, *Some Remarks on Pseudo-random Sequences*, Mathematica Slovaca **to appear** (1994).
53. L.P. Yarolslavsky, *Digital Picture Processing*, Springer-Verlag, Berlin Heidelberg New York Tokyo, 1985.

Contents