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 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.

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 $m = 5^s$.

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.

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.

The main result of my thesis is Theorem 3.36, which is a solution of a problem proposed by Robert Tichy.

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 Herendi [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 1281.

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 give 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 of Herendi, Siegl and Tichy [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 Herendi and Pethő [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 $N(I)$.*

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, 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 1.10. *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*

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

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*

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

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*

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

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 $a_0, \ldots, a_{d-1}$ with initial values $u_0, \ldots, u_{d-1}$ and let $P \subseteq R$ be a prime ideal. Let*

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

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

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

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 this dissertation.

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 $a_{s,0}, \ldots, a_{s,d_P(u,s)-1}$ 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 3rd chapter is a generalization of Herendi [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]).

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 $r \in R \setminus P$.*

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 $p \cdot r \equiv 1 \mod P^s$.*

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 $\lambda'_i \notin P$.

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 $j = 1 \ldots r$.

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 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 this 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.*

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 $\mod P^s$*.*

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.*

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

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* $\mod P^s$*.*

Remark 2.15. *Let $s < s'$ and suppose that $b_1, \ldots, b_d \in V$ is a semi-basis* $\mod P^s$*. This $b_1, \ldots, b_d$ is also a semi-basis* $\mod P^{s'}$*, otherwise it would be strongly dependent* $\mod P^{s'}$*, 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 $\mod P^s$ *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* $\mod P^s$*. If $b \in V$, then there exist $\lambda_1, \ldots, \lambda_d \in R$ and $p \in P^{s-1}$ such that*

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

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.

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* $\operatorname{lcm}(Q_1, Q_2)$.

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.*

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.*

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* $\operatorname{lcm}(Q_u, Q_v)$.

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.*

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

and the sequence has no preperiod.

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.*

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

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

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 3.17. *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*

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

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

$$u \equiv u^{(1)} + u^{(2)} \mod P^s \ ,$$
$$u^{(2)} \equiv 0 \mod P^t \ ,$$
$$T(u^{(1)}) \leq t \ ,$$
$$d(u^{(1)}) = d(u, t)$$
$$\textit{and}$$
$$d(u^{(2)}) \leq 2d(u) \ .$$

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 3.21. *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

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

The following theorem is fundamental:

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 $N(P) = \pi$.

We can formulate here an important result 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 $n, m, l, q \geq 0$.

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

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

As a consequence of the above results, if s is greater than a given bound, then 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

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

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

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

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

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

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

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

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}.

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

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

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

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

Remark 3.35. *The following theorem is a solution of a problem proposed by R. Tichy. This 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 $s \in \mathbb{N}$.

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 construction of uniformly distributed linear recurring sequences with arbitrary large period length. The fundamental application of such sequences is the construction of pseudo-random number generators.

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]. □

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]

We can 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*

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

The following proposition shows the distinguished 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.*

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.

Remark 4.19. *The statement of the lemma 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

$$\begin{aligned} P_1(x) &= P(x) \ , \\ P_2(x) &= P(x) - 2 \ , \\ P_3(x) &= P(x) - 2x \ , \\ P_4(x) &= P(x) - 2x - 2 \end{aligned}$$

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 $s \in \mathbb{N}$.

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.

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 Herendi, Siegl and Tichy [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*

$$D_N(\xi, \lambda, \mathfrak{I}) \leq D_N(\xi, \lambda, \mathfrak{C}) \leq (4k^{3/2} + 1) D_N(\xi, \lambda, \mathfrak{I})^{1/k}$$

Proof. See e.g. Theorem 1.6 in [23]. □

Remark 5.4. *Using the general inequality of Niederreiter and Wills* [33]*, we obtain*

$$\begin{aligned} &D_n\left(\bar{\eta}^{(m)}, \mu^{(m)}, \mathfrak{J}^{(m)}\right) \\ &\leq (4(k+m-1)+1)\left(D_n\left(\bar{\xi}^{(k+m-1)}, \lambda^{(k+m-1)}, \mathfrak{J}^{(k+m-1)}\right)\right)^{\frac{1}{k+m-1}} \ . \end{aligned} \tag{5.8}$$

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 $\mathbb{R}^k$.

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

$$D_n\left(\eta, \gamma, \mathfrak{I}\right) \leq \left(4k^{\frac{3}{2}} + 1\right) D_n\left(\bar{\xi}^{(k)}, \lambda^{(k)}, \mathfrak{I}^{(k)}\right)^{\frac{1}{k}} + \frac{33\sqrt{3}}{8\sqrt{k}} \ ,$$

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.

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.

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 Herendi and Pethő [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

$$u_n = u_{n-1} + au_{n-2} \quad \text{for} \quad n \geq 2 \ ,$$

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 $0 \leq k \leq n$. With the previous definitions*

$$u_n u_{k-1} = u_{n-1} u_k - (-1)^k a^k u_{n-k-1} \ .$$

Lemma 6.2. *Let $0 < k \leq n$ and u_n as before. Then*

$$u_n = u_{n-k} u_k + a u_{n-k-1} u_{k-1} \ .$$

Corollary 6.3. *Let $n \geq 1$. Then*

$$u_{n+2} = u_3 u_n - a^2 u_{n-2} \ .$$

Lemma 6.4. *Let R be a unique factorization domain, $n \in \mathbb{N}$ and let u be as above. Then*

$$\gcd(a, u_n) = 1 \ .$$

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*

$$\gcd\left(u_{n-1}, u_{k-1}\right) = u_{m-1} \ .$$

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*

$$\deg\left(F_n(x)\right) = \left[\frac{n}{2}\right] \ .$$

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 $k \in \mathbb{N}$.

Lemma 6.12. *The roots of $F_n(x)$ are*

$$-\frac{\xi_{n+1}^j}{\left(\xi_{n+1}^j+1\right)^2}\ ,$$

where $1 \le j \le \left[\frac{n}{2}\right]$ and ξ_{n+1} is an $n+1$-th primitive root of unity.

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. *We ca prove 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*

$$u_n = u_{n-1} - \frac{1}{4}u_{n-2} \quad \textit{for} \quad n \ge 2\ ,$$

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

$$F_n\left(-\frac{1}{4}\right) = u_n = (n+1)\left(\frac{1}{2}\right)^n \quad \textit{for all} \quad n \in \mathbb{N}\ .$$

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* $\{-1, -\frac{1}{2}, -\frac{1}{3}\}$.

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 6.20. *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

$$\delta_{0n} = \begin{cases} 0, & \textit{if } n = 0 \\ 1, & \textit{if } n \neq 0 \ . \end{cases}$$

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 6.23. *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.)

Lemma 6.24. *Let $n \geq 1$. Then*

$$f_{n+2}(x,y) = (2x+y) \cdot f_n(x,y) - x^2 \cdot f_{n-2}(x,y) \ .$$

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].

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

$$A = a \cdot \left(b^{\chi(n-2)} \cdot f_{n-2}\left(a, b^2\right) - B \cdot b^{\chi(k-2)} \cdot f_{k-2}\left(a, b^2\right)\right) \ .$$

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*

$$x^2 - bx - a \mid x^n - Bx^k - A \ .$$

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

$$b^{\chi(k-1)} f_{k-1}(a, b^2) \neq 0 \ .$$

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 $|b| \neq 1$.

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 $a, b \in \mathbb{Z}$.

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).

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].

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.

The author's publications not cited in the present work

[H1] A. Fazekas, T. Herendi, *Methods and Applications of Digital Image Processing*, Bulletins of Applied Math. **778** (1991), 369-377.
[H2] A. Fazekas, T. Herendi, *Thinning Algorithms in Digital Picture Processing*, Bulletins of Applied Math. **860** (1993), 301-306.
[H3] P. Grabner, T. Herendi, R.F. Tichy, *Fractal Digital Sums and Codes*, Applicable Algebra in Engineering, Communication and Computing **8** (1997), 33-39.
[H4] Hajdu L. és Herendi T., *Explicit bounds for the solutions of elliptic equations with rational coefficients*, J. Symbolic Computation **25** (1998), 361-366.