Journal de Théorie des Nombres
de Bordeaux **13** (2001), 303–314

Prime divisors of linear recurrences and Artin's primitive root conjecture for number fields

par Hans ROSKAM

Résumé. Soit S une suite définie par une récurrence linéaire entière d'ordre $k \geq 3$. On note P_S l'ensemble des nombres premiers qui divisent au moins l'un des termes de S. Nous donnons une approche heuristique du problème selon lequel P_S admet ou non une densité naturelle, et montrons que certains aspects de ces heuristiques sont corrects. Sous l'hypothèse d'une certaine généralisation de la conjecture d'Artin pour les racines primitives, nous montrons que P_S possède une densité asymptotique inférieure pour toute suite S "générique". Nous donnons en illustration des exemples numériques.

Abstract. Let S be a linear integer recurrent sequence of order $k \geq 3$, and define P_S as the set of primes that divide at least one term of S. We give a heuristic approach to the problem whether P_S has a natural density, and prove that part of our heuristics is correct. Under the assumption of a generalization of Artin's primitive root conjecture, we find that P_S has positive lower density for 'generic' sequences S. Some numerical examples are included.

1. Introduction

An integer sequence $S = \{x_n\}_{n=1}^{\infty}$ is said to satisfy a linear recurrence of order k, if there exist integers $a_1, a_2, \ldots, a_k$ such that

$$x_{n+k} = \sum_{i=1}^{k} a_i x_{n+k-i} \qquad \forall\, n \in \mathbf{Z}_{\geq 1}.$$

If such a sequence S does not satisfy a linear recurrence of order smaller than k, we say that S is a linear recurrent sequence of order k. In this case the x_n can be given as an exponential expression in the roots of the characteristic polynomial $f = X^k - \sum_{i=1}^{k} a_i X^{k-i} \in \mathbf{Z}[X]$ of the recurrence.

Manuscrit reçu le 1er novembre 1999.

For example, if f is separable with roots $\{\alpha_i\}_{i=1}^k$, we have

$$x_n = \sum_{i=1}^{k} c_i \alpha_i^n \qquad \forall\, n \in \mathbf{Z}_{\geq 1}, \tag{1}$$

where $c_1, \ldots, c_k \in \mathbf{Q}(\alpha_1, \ldots, \alpha_k)$ are determined by the initial values $\{x_n\}_{n=1}^k$.

Associated to a linear integer recurrent sequence S is the set P_S of primes dividing the sequence, where a prime p is said to divide the sequence if p divides some term of the sequence. We say that S is *degenerate* if the associated characteristic polynomial is either inseparable or has two different roots whose quotient is a root of unity. If S is degenerate, the set P_S is possibly finite. The fact that P_S is infinite for non-degenerate linear recurrent sequences S of order 2 is often attributed to Ward [15]. However, already in 1921 Pólya [10] proved that for *all* non-degenerate linear recurrent sequences S of order $k \geq 2$, the set P_S is infinite. His proof shows that a finite set P_S contradicts the growth rate of S.

Pólya's method seems inadequate to determine the 'size' of P_S. In particular, it does not allow us to decide whether P_S has a density $\delta(P_S)$ inside the set of all primes. Almost all results on the existence and value of $\delta(P_S)$ are for second order linear recurrent sequences S. In this second order case, the method of proof depends on two properties of the sequence: whether the sequence is 'torsion' [1, 4, 6, 9] or non-torsion [13], and whether the characteristic polynomial is reducible over $\mathbf{Q}$ [1, 4, 9, 13] or irreducible [6].

Essentially nothing is known for sequences of order larger than 2. The methods for second order sequences can be made to work in some very special cases: there exist higher order linear recurrent sequences having a set of *maximal* prime divisors of positive density [1]. Ward [16] introduced the term *maximal* prime divisors of a k-th order linear recurrent sequence for those primes that divide $k-1$ consecutive terms of the sequence, but do not divide all terms.

In this paper we focus on linear recurrent sequences S of order $k \geq 3$ whose associated characteristic polynomial is separable. Unfortunately, we are not able to prove that the set P_S of primes dividing such a sequence has a density. However, for a large class of linear recurrent sequences we can prove that P_S has positive lower density, if we assume a generalization of Artin's conjecture on primitive roots.

The paper is organized as follows. In section 2 we give a different characterization of the set P_S. This characterization is used in section 3, to give a heuristic approach to the problem whether the set P_S contains a set of positive density. Section 3 also contains a theorem stating that part of the heuristics is correct. This theorem, combined with a generalization of Artin's conjecture on primitive roots, implies that P_S has positive lower density for 'generic' sequences S. After proving the theorem in section 4, we give some numerical examples in section 5.

2. Reformulation of the problem

Let $S = \{x_n\}_{n=1}^{\infty}$ be an integer sequence satisfying the linear recurrence of order $k \geq 2$ with separable characteristic polynomial

$$f = X^k - \sum_{i=1}^{k} a_i X^{k-i} = \prod_{i=1}^{k} (X - \alpha_i) \in \mathbf{Z}[X].$$

The sequence S is an element of V_f, the set of all sequences of algebraic numbers satisfying the linear recurrence with characteristic polynomial f. By defining addition and scalar multiplication of sequences componentwise, the set V_f becomes a $\bar{\mathbf{Q}}$-vectorspace. As f is separable, the sequences $\{\alpha_1^n\}_{n=1}^{\infty}, \ldots, \{\alpha_k^n\}_{n=1}^{\infty}$ form a $\bar{\mathbf{Q}}$-basis for V_f, and there exist $c_1, \ldots, c_k \in \bar{\mathbf{Q}}$ such that $x_n = \sum_{i=1}^{k} c_i \alpha_i^n$ for all positive integers n. The absolute Galois group $G_{\mathbf{Q}}$ of $\mathbf{Q}$ permutes the α_i's and acts trivially on the integers x_n. Using that the sequences $\{\{\alpha_i^n\}_{n=1}^{\infty}\}_{i=1}^{k}$ form a basis for V_f, we find that the set $\{c_i\}_{i=1}^{k}$ is $G_{\mathbf{Q}}$-invariant. Moreover, each $\sigma \in G_{\mathbf{Q}}$ induces the same permutation on the sets $\{c_i\}_{i=1}^{k}$ and $\{\alpha_i\}_{i=1}^{k}$.

Now let α denote the residue class of X in the free $\bar{\mathbf{Q}}$-algebra $A = \bar{\mathbf{Q}}[X]/(f)$ of rank k. By the Chinese remainder theorem, the c_i's determine a unique $c \in A$ such that $c(\alpha_i) = c_i$ for $i = 1, \ldots, k$. Because of the last remark of the previous paragraph, $G_{\mathbf{Q}}$ acts trivially on c. We conclude that there exists a unique $c \in \mathbf{Q}[X]/(f)$ such that

$$x_n = \mathrm{Tr}_{A/\bar{\mathbf{Q}}}(c\alpha^n) \qquad \forall n \in \mathbf{Z}_{\geq 1}. \tag{2}$$

Denote the set of primes that divide the sequence S by P_S. A prime p is an element of P_S if and only if there exists an integer n such that

$$\mathrm{Tr}_{A/\bar{\mathbf{Q}}}(c\alpha^n) \equiv 0 \bmod p\mathbf{Z}.$$

In order to interchange the trace-map and the reduction modulo $p\mathbf{Z}$, we choose an integer $d \neq 0$ such that $cd \in \mathbf{Z}[X]/(f)$ and define $R = \mathbf{Z}[\frac{1}{d}]$. The (maximal) primes of the ring R are of the form pR, with p a rational prime not dividing d. In the following we disregard the finitely many primes dividing d. This restriction has no effect on the existence or value of the density of P_S.

The elements $c\alpha^n$ are contained in $\mathcal{O} = R[X]/(f)$, a free R-algebra of rank k. As the trace is stable under base change and the $\bar{\mathbf{Q}}$-algebras A and $\mathcal{O} \otimes_R \bar{\mathbf{Q}}$ are isomorphic, we can write equation (2) as

$$x_n = \mathrm{Tr}_{\mathcal{O}/R}(c\alpha^n) \qquad \forall n \in \mathbf{Z}_{\geq 1}. \tag{3}$$

To compute x_n modulo a prime p of R, we tensor the trace-map $\mathrm{Tr} : \mathcal{O} \to R$ with R/pR over R and obtain the trace-map $\mathrm{Tr} : \mathcal{O}/p\mathcal{O} \to R/pR$.

We find that a prime p of R divides the sequence if and only if there exists an integer n such that

$$\mathrm{Tr}_{(\mathcal{O}/p\mathcal{O})/\mathbf{F}_p}(\bar{c}\bar{\alpha}^n) = 0,$$

where the bar means reduction modulo $p\mathcal{O}$. In other words, if H denotes the kernel of the trace map $\mathrm{Tr} : \mathcal{O}/p\mathcal{O} \to \mathbf{F}_p$, we have the following criterion for a prime p of R to divide the sequence:

$$p \in P_S \Longleftrightarrow \bar{c}\langle\bar{\alpha}\rangle \cap H \neq \emptyset. \tag{4}$$

This characterization hints to why the determination of P_S is difficult. The group H is an *additive* subgroup of the ring $\mathcal{O}/p\mathcal{O}$, whereas, for almost all primes, $\bar{c}\langle\bar{\alpha}\rangle$ is a coset of the *multiplicative* subgroup $\langle\bar{\alpha}\rangle \subset (\mathcal{O}/p\mathcal{O})^*$. Such a mixture of an additive and multiplicative structure is notoriously difficult to study.

3. Heuristic approach

In this section we let p range over the primes of R and predict the 'probability' that p divides a fixed linear recurrent sequence S. If this 'probability' is positive, we expect P_S to be a set of primes of positive density inside the set of all primes. By the equivalence (4) of section 2, the likelihood that p divides S will depend on the size of the subgroup $\langle\bar{\alpha}\rangle \subset (\mathcal{O}/p\mathcal{O})^*$. In the extreme case that $\bar{\alpha}$ generates $(\mathcal{O}/p\mathcal{O})^*$, the intersection $\bar{c}\langle\bar{\alpha}\rangle \cap H$ is non-empty and p divides the sequence. To make the importance of the size of $\langle\bar{\alpha}\rangle$ more explicit, we fix a prime p of R such that $c\alpha$ is a unit modulo $p\mathcal{O}$. As the trace-map is surjective, its kernel $H \subset \mathcal{O}/p\mathcal{O}$ has index p. The probability for a randomly chosen $x \in \mathcal{O}/p\mathcal{O}$ to have non-zero trace is $1-\frac{1}{p}$. The elements in the coset $\bar{c}\langle\bar{\alpha}\rangle \subset (\mathcal{O}/p\mathcal{O})^*$ are not randomly chosen elements of $\mathcal{O}/p\mathcal{O}$. However, if we let p range over the primes of R, it seems plausible that the additive and multiplicative structure of the ring $\mathcal{O}/p\mathcal{O}$ are 'independent'. Therefore, we assume that as p varies, the 'probability' that an element in the coset $\bar{c}\langle\bar{\alpha}\rangle$ has non-zero trace is $1 - \frac{1}{p}$. As a further simplification, we assume the 'probability' that *all* elements in $\bar{c}\langle\bar{\alpha}\rangle$ have non-zero trace, to be equal to $(1 - \frac{1}{p})^{\#\bar{c}\langle\bar{\alpha}\rangle}$. Note that these assumptions are wrong for $k = 1$. In this case, the trace-map is the identity, and none of the elements in $(\mathcal{O}/p\mathcal{O})^* = \mathbf{F}_p^*$ has zero trace. With the above assumptions and the equivalence (4), we conclude that the 'probability' that a prime p does *not* divide a fixed linear recurrent sequence is approximated by

$$(1 - \frac{1}{p})^{\#\langle\bar{\alpha}\rangle}.$$

In order to obtain a set of primes of positive density that *do* divide the sequence, we need a set of positive density, consisting of primes p for which this probability is 'small', or, equivalently, for which the order of $\bar{\alpha} \in (\mathcal{O}/p\mathcal{O})^*$ is 'large'.

For an integer $a \neq 0$, the order of $\bar{a} \in \mathbf{F}_p^*$ divides $p-1$. In 1927, Emil Artin conjectured that if a is not equal to -1 or a square, the set of primes p for which the order of $\bar{a} \in \mathbf{F}_p^*$ equals $p-1$ has positive density. More generally, we expect that for each $h \in \mathbf{Z}_{\geq 1}$, the set T_h of primes p for which the order of $\bar{a} \in \mathbf{F}_p^*$ is $(p-1)/h$, has a density $\delta(T_h)$. Note that $\delta(T_h)$ is not positive for all a and $h \in \mathbf{Z}_{\geq 1}$; if a is a square, there are no odd primes p for which $\bar{a} \in \mathbf{F}_p^*$ has order $p-1$. However, we do expect the equality $\sum_{h=1}^{\infty} \delta(T_h) = 1$ to hold. In other words, we expect that for 'most' primes p, the order of a modulo p is 'almost' maximal. These conjectures are still open, but have been proved under the assumption of the generalized Riemann hypothesis [5, 7, 14].

To adapt Artin's conjecture to our situation, we first need an upper bound for the order of $\bar{\alpha} \in (\mathcal{O}/p\mathcal{O})^*$. The trivial upper bound for this order is the exponent $e(p)$ of $(\mathcal{O}/p\mathcal{O})^*$. The value of $e(p)$ as function of the prime p depends on the splitting type of the characteristic polynomial f modulo p. More precisely, for primes p not dividing the discriminant of f, we have $e(p) = \mathrm{lcm}_d(p^d - 1)$, with d ranging over the degrees of the irreducible factors of $\bar{f} \in \mathbf{F}_p[X]$. Now, let T be the set of primes with a fixed splitting type. We say that α, or, equivalently, f, satisfies the generalized Artin conjecture for primitive roots, if the following holds.

For each $h \in \mathbf{Z}_{\geq 1}$, the set T_h of primes $p \in T$ for which the order of $\bar{\alpha} \in (\mathcal{O}/p\mathcal{O})^*$ is $e(p)/h$, has a density $\delta(T_h)$. Moreover, we have $\sum_{h=1}^{\infty} \delta(T_h) = \delta(T)$.

Artin's original conjecture excludes the integers ± 1. In our general setting, there are more α's for which the above conjecture does not hold. However, we expect the conjecture to hold for 'generic' α. As it is not our prime interest to classify the exceptional α's, we do not specify what we mean by 'generic'. Instead we give an example of a non-generic α. Assume f does not factor over $\mathbf{Q}$ as a product of linear polynomials. By Chebotarev's density theorem, the set T of primes p for which f does not split completely into linear factors modulo p, has a positive density. For $p \in T$, the exponent $e(p)$ is at least $p^2 - 1$. Now assume in addition that α^k is rational, for some fixed $k \in \mathbf{Z}_{\geq 1}$. The order of $\bar{\alpha} \in (\mathcal{O}/p\mathcal{O})^*$ is at most $k(p-1)$, so T_h is finite for all $h \in \mathbf{Z}_{\geq 1}$. We find that $\sum_{h=1}^{\infty} \delta(T_h) = 0$ is strictly less than $\delta(T)$, and the above conjecture does not hold.

Now we return to our linear recurrent sequence S of order $k \geq 2$. Assume that the associated characteristic polynomial of S satisfies the generalized Artin conjecture. For the following, we distinguish two cases; either f splits into distinct linear factors modulo p, or not. In the former case we say that p is a *splitting prime* or that p *splits completely*.

First we take for T the set of primes that split completely. The set T has positive density by Chebotarev's density theorem For $p \in T$, the group

$(\mathcal{O}/p\mathcal{O})^*$ is isomorphic to $\prod_{j=1}^k \mathbf{F}_p^*$, and has exponent $e(p) = p-1$. By assumption there exists $h \in \mathbf{Z}_{\geq 1}$ such that the set T_h of primes $p \in T$ for which $\bar{\alpha} \in (\mathcal{O}/p\mathcal{O})^*$ has order $(p-1)/h$, has a positive density. According to our heuristics, the 'probability' that $p \in T_h$ does *not* divide the sequence is $(1-\frac{1}{p})^{(p-1)/h}$. For $p \to \infty$ this expression converge to $e^{-1/h}$, which lies strictly between 0 and 1. Therefore, we expect that T_h contains two subsets of positive lower density, one consisting of primes that *do* divide the sequence, and one consisting of primes that do *not* divide the sequence. As a consequence, it seems plausible that the set of primes in T that divide S has a positive lower density, strictly less than 1. Note that although the above formula for the 'probability' does give us an indication of what to expect, it does not pretend to give a precise value for the density of the set of primes in T_h that divide S. Therefore, our heuristics do not predict the existence of the density of the set of primes in T that divide S.

Now, let T be the set of primes that do not split completely. For $h \in \mathbf{Z}_{\geq 1}$, we define T_h as the set of primes $p \in T$ for which the order of $\bar{\alpha} \in (\mathcal{O}/p\mathcal{O})^*$ is equal to $e(p)/h$. As f does not split completely modulo $p \in T$, we have $e(p) \geq p^2 - 1$. Using our heuristic formula, we expect the 'probability' that $p \in T_h$ does *not* divide S to be at most $(1-\frac{1}{p})^{(p^2-1)/h}$. This expression converges exponentially to 0, for $p \to \infty$. Therefore, for all $h \in \mathbf{Z}_{\geq 1}$, the subset of T_h of primes that do *not* divide the sequence, should have zero density. According to our generalization of Artin's conjecture, the density of $\cup_{h \leq n} T_h$ gets arbitrarily close to $\delta(T)$, for $n \to \infty$. As a conclusion, we expect the set of primes that do not split completely and that do *not* divide the sequence to have zero density.

Up to now, we discussed linear recurrent sequences of any order $k \geq 2$. The theorem below and the data in section 5 support the above heuristics for linear recurrent sequences of order $k \geq 3$. However, for a specific linear recurrent sequence S of order 2 with irreducible polynomial, the above heuristics are proved to be false. Let $S = \{x_n\}_{n=1}^{\infty}$ be the linear recurrent sequence with irreducible characterisitic polynomial $f = X^2 - 5X + 7$ and initial values $x_1 = 1$ and $x_2 = 2$. Let α and $\bar{\alpha}$ be the roots of f and denote by $\mathcal{O}$ the ring of integers of $\mathbf{Q}(\alpha)$. Lagarias [6] showed that a prime p divides S if and only if the order of $\alpha/\bar{\alpha} \in (\mathcal{O}/p\mathcal{O})^*$ is divisible by 3. This condition is equivalent with certain spitting conditions for p in certain number fields. Using Chebotarev's density theorem, Lagarias showed that the set of primes that do not split completely in $K/\mathbf{Q}$ and that do *not* divide S has *positive* density. According to our heuristics, this set should have zero density.

Let S be a linear recurrent sequence of order $k \geq 3$. Recall from section 2 that α denotes the residue class of X in the ring $\mathcal{O} = \mathbf{Z}[\frac{1}{d}][X]/(f)$, where

d is some fixed integer. Define for each $h \in \mathbf{Z}_{\geq 1}$ the set

$$T_h = \{p : f \text{ is irreducible modulo } p, \text{ and } [(\mathcal{O}/p\mathcal{O})^* : \langle\bar{\alpha}\rangle] = h\}.$$

Theorem. *Let S be a linear recurrent sequence of order $k \geq 3$, and define for each positive integer h the set T_h as above. For every positive integer h, all but finitely many primes in T_h divide S.*

We will prove this theorem in the next section. The main idea of the proof is to relate the primes $p \in T_h$ that divide S to the existence of $\mathbf{F}_p$-rational points on some projective algebraic variety defined over $\mathbf{F}_p$. For large p, the existence of these points is guaranteed by a result of Lang and Weil.

The theorem does not imply that P_S contains a set of positive density. There are two problems. First of all the set T of primes p for which $\bar{f} \in \mathbf{F}_p[X]$ is irreducible might be empty, for example if f is reducible over $\mathbf{Q}$. If f is irreducible, a necessary and sufficient condition for T to have positive density, is the existence of a k-cycle in the Galois group of f. Namely, suppose f is irreducible modulo the prime p. The decomposition group of a prime above p in a normal closure of $\mathbf{Q}[X]/(f)$ acts transitively on the roots of f, and therefore contains a k-cycle. The fact that the existence of a k-cycle is sufficient for T to have positive density follows from Chebotarev's density theorem.

Much more difficult is the question whether there exists $h \in \mathbf{Z}_{\geq 1}$ such that T_h has positive density. An affirmative answer to this question is precisely the generalization of Artin's conjecture that we discussed above. In order to conclude that P_S has positive lower density, we need the following precise version of this conjecture.

Generalized Artin conjecture: *Let $f \in \mathbf{Z}[X]$ be an irreducible monic polynomial, α a root of f, and define $K = \mathbf{Q}(\alpha)$ with ring of integers $\mathcal{O}_K$. Furthermore, let T be the set of primes that are inert in $K/\mathbf{Q}$ and define for each $h \in \mathbf{Z}_{\geq 1}$, the set T_h of primes $p \in T$ for which the subgroup $\langle\bar{\alpha}\rangle \subset (\mathcal{O}_K/p\mathcal{O}_K)^*$ has index h.*
Then T_h has a natural density $\delta(T_h)$ for all $h \in \mathbf{Z}_{\geq 1}$. Moreover, we have the equality $\sum_{h=1}^{\infty} \delta(T_h) = \delta(T)$.

As we saw before, although it happens that the conjecture fails to hold for specific α, we expect the conjecture to hold for 'generic' α. Based on computer calculations for quadratic polynomials, Brown and Zassenhaus made a similar conjecture [2]. Under some mild assumptions on the polynomial f, they conjectured that the set T_1 has positive density.

The generalized Artin conjecture has been proved for integers $\alpha \notin \{0, \pm 1\}$, or, equivalently, for linear polynomials f, under the assumption of the generalized Riemann hypothesis [5, 7, 14]. Under the same assumption, we proved [12] that part of the conjecture holds for irreducible quadratic polynomials f. Unfortunately, we are not able to prove the generalized Artin conjecture for a single polynomial of degree at least 3, not even under the assumption of the generalized Riemann hypothesis.

Corollary. *Let S be a linear recurrent sequence of order $k \geq 3$. Assume the associated characteristic polynomial satisfies the generalized Artin conjecture, and contains a k-cycle in its Galois group. Then P_S contains a set of positive density.*

Proof. Let α be a root of the characteristic polynomial f, and let $\mathcal{O}_K$ be the ring of integers of the number field $K = \mathbf{Q}(\alpha)$. For all primes p not dividing d, the ring $\mathcal{O}/p\mathcal{O}$ is isomorphic to $\mathcal{O}_K/p\mathcal{O}_K$. By the assumption on f, we conclude that T_h has a density $\delta(T_h)$ for all positive integers h. According to the theorem, the density of the set $T_{S,h}$ of primes $p \in T_h$ that divide S is equal to $\delta(T_h)$. Denote the upper density and lower density of $T_S = T \cap P_S$ by $\bar{\delta}(T_S)$ and $\underline{\delta}(T_S)$ respectively. Using the above remarks, we find:

$$\delta(T) \geq \bar{\delta}(T_S) \geq \underline{\delta}(T_S) \geq \sum_{h=1}^{\infty} \delta(T_{S,h}) = \sum_{h=1}^{\infty} \delta(T_h) = \delta(T)$$

We conclude that the set T_S has a density and moreover we have $\delta(T_S) = \delta(T)$. As the Galois group of f contains a k-cycle, this density is positive. □

4. Proof of the theorem

As in section 2, we choose an integer $d \neq 0$ such that $x_n = \mathrm{Tr}_{\mathcal{O}/R}(c\alpha^n)$, where $\mathcal{O} = R[X]/(f)$ is a free algebra over $R = \mathbf{Z}[\frac{1}{d}]$, and $c \in \mathcal{O}$ is uniquely determined by $\{x_i\}_{i=1}^{k}$. Fix $h \in \mathbf{Z}_{\geq 1}$ and define the set

$$T_{S,h} = \{p \in T_h : p \text{ divides } S\} = P_S \cap T_h.$$

Let $p \in T_h$ be a prime not dividing d and write $\bar{\alpha}$ for the reduction of α modulo $p\mathcal{O}$. By assumption f is irreducible modulo p, and $\mathcal{O}/p\mathcal{O} = \mathbf{F}_p[\bar{\alpha}]$ is a field of order p^k. As $(\mathcal{O}/p\mathcal{O})^*$ is cyclic, the subgroup generated by $\bar{\alpha}$ consists of the h-th powers in $(\mathcal{O}/p\mathcal{O})^*$, and we find

$$\langle\bar{\alpha}\rangle = \big\{(\sum_{i=1}^{k} x_i\bar{\alpha}^i)^h : x_1, \ldots, x_k \in \mathbf{F}_p \text{ not all } 0\big\}.$$

Together with the equivalence (4) in section 2, this yields the following characterization:

$$(5) \qquad p \in T_{S,h} \Longleftrightarrow \begin{cases} \exists\ x_1, \ldots, x_k \in \mathbf{F}_p \text{ not all 0 such that} \\ \mathrm{Tr}_{(O/p\mathcal{O})/\mathbf{F}_p}\big(\bar{c}\,(\sum_{i=1}^{k} x_i\bar{\alpha}^i)^h\big) = 0. \end{cases}$$

We will show that if p is large enough, then the right hand side of (5) is satisfied. This implies that all but finitely many primes in T_h divide S, and the theorem is proved.

By extending scalars, we find that $\mathcal{O}[X_1, \ldots, X_k]$ is a free $R[X_1, \ldots, X_k]$-algebra. Define the homogeneous polynomial

$$F_h = \mathrm{Tr}_{\mathcal{O}[X_1,\ldots,X_k]/R[X_1,\ldots,X_k]}\big(c\,(\sum_{i=1}^{k} X_i\alpha^i)^h\big) \in R[X_1, \ldots, X_k].$$

Note that F_h is independent of the prime p. The coefficient $\mathrm{Tr}_{\mathcal{O}/R}(c\alpha^h)$ of X_1^h in F_h is the h-th term of the sequence S. If this coefficient is zero, then all primes divide S and the theorem is proved. Therefore, we assume that $\mathrm{Tr}_{\mathcal{O}/R}(c\alpha^h)$ is non-zero, so F_h is homogeneous of degree h. Let $V_h \subset \mathbf{P}^{k-1}(\bar{\mathbf{Q}})$ be the projective algebraic set defined by F_h. The reduction $\bar{V}_h$ of V_h modulo p is given by the polynomial

$$\bar{F}_h = \mathrm{Tr}_{(\mathcal{O}/p\mathcal{O})[X_1,\ldots,X_k]/\mathbf{F}_p[X_1,\ldots,X_k]}\big(\bar{c}\,(\sum_{i=1}^{k} X_i\bar{\alpha}^i)^h\big) \in \mathbf{F}_p[X_1, \ldots, X_k].$$

For $x_1, \ldots, x_k \in \mathbf{F}_p$, the equation on the right hand side of the equivalence (5) becomes $\bar{F}_h(x_1, \ldots, x_k) = 0$, so we arrive at

$$p \in T_{S,h} \Longleftrightarrow \bar{V}_h(\mathbf{F}_p) \neq \emptyset, \tag{6}$$

where $\bar{V}_h(\mathbf{F}_p)$ denotes the set of $\mathbf{F}_p$-rational points of $\bar{V}_h$.

In order to prove that $\bar{V}_h$ is a non-singular projective variety, we let $W_h \subset \mathbf{P}^{k-1}(\bar{\mathbf{F}}_p)$ be the projective algebraic set defined by

$$G_h = \sum_{i=1}^{k} \bar{c}^{\,p^{i-1}} Y_i^h \in (\mathcal{O}/p\mathcal{O})[Y_1, \ldots, Y_k].$$

If $p \nmid h$ and $\bar{c} \neq 0$, then the partial derivatives of G_h do not vanish simultaneously on $\mathbf{P}^{k-1}(\bar{\mathbf{F}}_p)$, and W_h is a smooth projective hypersurface of dimension $k-2$. As k is at least 3, the intersection of two different irreducible components of W_h is non-empty by [3, Theorem 7.2 on page 48]. However, the points of such an intersection are singular points of W_h. Because W_h is smooth, this proves that W_h is absolutely irreducible.

Note that if k equals 2, then $W_h(\bar{\mathbf{F}}_p)$ consists of h points, and is not absolutely irreducible.

The varieties W_h and $\bar{V}_h$ are isomorphic over $\mathcal{O}/p\mathcal{O}$. Namely, we can define a morphism $\phi : \bar{V}_h \to W_h$ by the equations

$$Y_i = \sum_{j=1}^{k} X_j \bar{\alpha}^{jp^{i-1}} \quad \text{for } 1 \leq i \leq k.$$

The determinant of ϕ is equal to $\mathrm{N}(\bar{\alpha})^k$ times the Vandermonde determinant of $\{\bar{\alpha}, \bar{\alpha}^p, \ldots, \bar{\alpha}^{p^k}\}$. As $\bar{\alpha} \in \mathcal{O}/p\mathcal{O}$ is of degree k over $\mathbf{F}_p$, the determinant is non-zero and ϕ is an isomorphism. We conclude that for all $p \in T_h$ that do not divide cdh, the algebraic set $\bar{V}_h$ is a smooth, absolutely irreducible hypersurface in $\mathbf{P}^{k-1}(\bar{\mathbf{F}}_p)$ of degree h.

The result of Lang and Weil [8, Theorem 1] yields the following estimate for the number of rational points of $\bar{V}_h$: there exists a constant C, depending on h and k only, such that for all primes $p \in T_h$ not dividing cdh we have

$$|\#\bar{V}_h(\mathbf{F}_p) - p^{k-2}| \leq Cp^{k-\frac{5}{2}}.$$

Note that instead of [8] one can also use the Weil-conjectures to obtain this estimate. We conclude that if $p \in T_h$ is large enough, then $\bar{V}_h(\mathbf{F}_p)$ is not empty and (6) implies that p divides S. This finishes the proof of the theorem.

5. Numerical examples

In the table below, we have collected some numerical data. For each of the five recurrences, there are two recurrent sequences. For each of these sequences, we determined how many of the 5133 primes up to $5 \cdot 10^4$ divide the sequence and ordered them by their splitting type. For example, for 853 primes up to $5 \cdot 10^4$, the polynomial $f = X^3 - 2X^2 + X - 6 \in \mathbf{F}_p[X]$ splits into three linear factors. Out of these 853 primes, 293 divide the sequence defined by f and the initial conditions $x_1 = 1, x_2 = -2$ and $x_3 = 5$. A 'mixed' splitting type just means that $f \in \mathbf{F}_p[X]$ factors as the product of a linear an a quadratic polynomial. The first 6 sequences have an irreducible characteristic polynomial with Galois group S_3, the symmetric group on 3 elements. For the next 2 sequences, the polynomial is irreducible with cyclic Galois group. The characteristic polynomial for the last two sequences factors over $\mathbf{Q}$ as a product of a linear and a quadratic factor.

For each of these sequences, the conclusions that we drew on heuristic arguments in section 3, seem to be correct. Almost all primes that do not split completely, divide the sequence, and out of the primes that split completely, a positive proportion does divide the sequence and a positive proportion does not.

The first two characteristic polynomials are related. If α is a root of $f = X^3 - 2X^2 + X - 6$, then $\beta = \alpha^6$ is a root of $g = X^3 - 254X^2 - 3311X - 46656$. In other words, the third and the fourth sequence are subsequences of the first and the second, respectively. Therefore, the first sequence has at least as many prime divisors as the third sequence. The heuristical arguments in section 3 explain why the first sequence has considerably more splitting prime divisors than the third sequence, and why both sequences have almost the same number of non-splitting prime divisors. First we note that as α

and β define isomorphic number fields, the splitting type of f modulo p is the same as that of g modulo p. Our heuristical model predicts that for any linear recurrent sequence S of order $k \geq 3$, almost all primes that do not split completely should divide S. In particular, almost all primes that do not split completely divide both the first and the third sequence. Now let p be a splitting prime, so the 'probability' that p does *not* divide either of the sequences is positive. If the order of $\bar{\alpha} \in (\mathcal{O}/p\mathcal{O})^*$ is not relatively prime to 6, the order of $\bar{\beta} = \bar{\alpha}^6$ is smaller than that of $\bar{\alpha}$. According to our heuristics, it is then more likely for p to divide the first sequence, than to divide the third. For example, there are no odd splitting primes p for which the order of $\bar{\beta} \in (\mathcal{O}/p\mathcal{O})^*$ is $p-1$. On the other hand, out of the set of primes that split completely, the primes p for which the order of $\bar{\alpha} \in (\mathcal{O}/p\mathcal{O})^*$ is $p-1$, have the largest 'probability' to divide the first sequence. Therefore, the number of splitting primes dividing the first sequence should be larger than the number of splitting primes dividing the third sequence.

splitting type:	Split	Mixed	Inert
$x_{n+3} = 2x_{n+2} - x_{n+1} + 6x_n$	853	2570	1707
$x_1 = 1,\ x_2 = -2,\ x_3 = 5$	293	2567	1707
$x_1 = 5,\ x_2 = 3,\ x_3 = 2$	290	2566	1707
$x_{n+3} = 254x_{n+2} + 3311x_{n+1} + 46656x_n$	853	2570	1707
$x_1 = 1,\ x_2 = -2,\ x_3 = 5$	159	2558	1707
$x_1 = 5,\ x_2 = 3,\ x_3 = 2$	156	2558	1707
$x_{n+3} = x_{n+2} + x_{n+1} + x_n$	839	2588	1704
$x_1 = 1,\ x_2 = 1,\ x_3 = 1$	519	2588	1704
$x_1 = 3,\ x_2 = -8,\ x_3 = 14$	332	2587	1704
$x_{n+3} = 3x_{n+2} + 18x_{n+1} - 13x_n$	1707	0	3425
$x_1 = 1,\ x_2 = 3,\ x_3 = -4$	914	0	3425
$x_1 = -7,\ x_2 = 5,\ x_3 = 2$	931	0	3424
$x_{n+3} = 5x_{n+2} - 11x_{n+1} + 10x_n$	2543	2589	0
$x_1 = 1,\ x_2 = 2,\ x_3 = 3$	1381	2585	0
$x_1 = 17,\ x_2 = 12,\ x_3 = -2$	1374	2586	0

We conclude with a few observations. As we can see from the fifth and the sixth sequence, the number of splitting primes dividing a linear recurrent seems to dependent not only on the characteristic polynomial, but also on the initial conditions. This can not be explained by our heuristics.

Our theorem is in fact empty for the fifth and sixth sequence. Namely, let α be a root of $f = X^3 - X^2 - X - 1$, and let p be a prime for which f is irreducible modulo p. As α has norm 1, the index $[(\mathcal{O}/p\mathcal{O})^* : \langle\bar{\alpha}\rangle]$ is at least $p-1$, and the set T_h is finite for all $h \in \mathbf{Z}_{\geq 1}$. This argument also shows that the generalized Artin conjecture does not hold for f. However, the data suggest that our heuristical conclusions on the number of prime divisors is still correct. This can be explained by the assumption that for 'most' primes p, the order of $\bar{\alpha} \in (\mathcal{O}/p\mathcal{O})^*$ is still 'as large as possible'. To be more precise, if we adapt our heuristics by replacing $e(p)$ by the exponent $\tilde{e}(p)$ of the kernel of the norm $\mathrm{N}\colon (\mathcal{O}/p\mathcal{O})^* \to \mathbf{F}_p$, we can draw the same conclusions as in section 3. For a generalization of Artin's conjecture for units in real quadratic fields, we refer to [11].

Finally we note that further numerical experiments seem to suggest that for the sequences S in the table, the splitting primes dividing S have a density. As an example, from the table we see that 34% of the 853 splitting primes up to $5 \cdot 10^4$ divide the first sequence. We computed that out of the first 853 splitting primes greater than $5 \cdot 10^4$, this percentage is 35%.

References

[1] C. BALLOT, *Density of prime divisors of linear recurrent sequences.* Mem. of the AMS **551** (1995).

[2] H. BROWN, H. ZASSENHAUS, *Some empirical observations on primitive roots.* J. Number Theory **3** (971),306–309.

[3] R. HARTSHORNE, *Algebraic geometry.* Springer-Verlag, New York, 1977.

[4] H. HASSE, *Über die Dichte der Primzahlen p, für die eine vorgegebene ganz-rationale Zahl a $\neq$ 0 von gerader bzw. ungerader Ordnung mod.p ist.* Math. Ann. **166** (1966), 19–23.

[5] C. HOOLEY, *On Artin's conjecture.* J. Reine Angew. Math. **225** (1967), 209–220.

[6] J.C. LAGARIAS, *The set of primes dividing the Lucas numbers has density* 2/3. Pacific J. Math. **118** (1985), 449–461; Errata Ibid. **162** (1994), 393–397.

[7] H.W. LENSTRA, JR, *On Artin's conjecture and Euclid's algorithm in global fields.* Inv. Math. **42** (1977), 201–224.

[8] S. LANG, A. WEIL, *Number of points of varieties in finite fields.* Amer. J. Math. **76** (1954), 819–827.

[9] P. MOREE, P. STEVENHAGEN, *Prime divisors of Lucas sequences.* Acta Arith. **82** (1997), 403–410.

[10] G. PÓLYA, *Arithmetische Eigenschaften der Reihenentwicklungen rationaler Funktionen.* J. Reine Angew. Math. **151** (1921), 99–100.

[11] H. ROSKAM, *A Quadratic analogue of Artin's conjecture on primitive roots.* J. Number Theory **81** (2000), 93–109.

[12] H. ROSKAM, *Artin's Primitive Root Conjecture for Quadratic Fields.* Accepted for publication in J. Théor. Nombres Bordeaux.

[13] P.J. STEPHENS, *Prime divisors of second order linear recurrences.* J. Number Theory **8** (1976), 313–332.

[14] S.S. WAGSTAFF, *Pseudoprimes and a generalization of Artin's conjecture.* Acta Arith. **41** (1982), 141–150.

[15] M. WARD, *Prime divisors of second order recurring sequences.* Duke Math. J. **21** (1954), 607–614.

[16] M. WARD, *The maximal prime divisors of linear recurrences.* Can. J. Math. **6** (1954), 455–462

Hans ROSKAM
Mathematisch Instituut
Universiteit Leiden
Postbus 9512, 2300 RA Leiden
The Netherlands
E-mail : roskam@math.leidenuniv.nl