New York Journal of Mathematics

New York J. Math. **25** (2019) 207–218.

Arithmetic properties of quadratic exponential polynomials

Igor E. Shparlinski and Umberto Zannier

ABSTRACT. Given $3n$ algebraic integers $\alpha_{i,\nu}$, $i = 1, \ldots, n$, $\nu = 0, 1, 2$, and an integer ideal $\mathfrak{q}$ in an algebraic number field K, we obtain several new bounds on the number of solutions to the congruence with a quadratic exponential polynomial

$$\sum_{i=1}^{n} \prod_{\nu=0}^{2} \alpha_{i,\nu}^{x^\nu} \equiv 0 \pmod{\mathfrak{q}}, \quad 1 \le x \le N.$$

We then apply these bounds to studying arithmetic properties of values of linear recurrence sequences on squares.

CONTENTS

1. Introduction

Motivated by the wealth of results of arithmetic properties of linear recurrence sequences (see [6, Chapter 6] and also [2, 12] for more recent results) we consider more general exponential polynomials. In particular, the class of sequences we study includes linear recurrence sequences evaluated on polynomial values of the argument.

Received October 12, 2018.

2010 *Mathematics Subject Classification.* 11B37, 11D61.

Key words and phrases. exponential polynomials, congruences, linear recurrence sequences.

I.S. was supported in part by the ARC Grant DP180100201.

ISSN 1076-9803/2019

Let $n \ge 3$ and let

$$U(x) = \sum_{i=1}^{n} \prod_{\nu=0}^{2} \alpha_{i,\nu}^{x^\nu} \tag{1.1}$$

be a quadratic exponential polynomial, where $\alpha_{i,\nu} \in \mathbb{Z}_K$, $i = 1, \ldots, n$, $\nu = 0, 1, 2$, are elements from the ring $\mathbb{Z}_K$ of algebraic integers in a fixed number field K. We note that $\alpha_{i,0}$ serve as coefficients, while $\alpha_{i,1}$ and $\alpha_{i,2}$ are bases of exponential and quadratic exponential functions, respectively, $i = 1, \ldots, n$.

For an integer ideal $\mathfrak{q}$ of $\mathbb{Z}_K$ and an integer N we denote

$$Q(N, \mathfrak{q}) = \#\{1 \le x \le N \ : \ U(x) \equiv 0 \pmod{\mathfrak{q}}\}.$$

We are interested in obtaining upper bounds of $Q(N, \mathfrak{q})$ and similar quantities. A similar question has been extensively studied in a simpler context of congruences with linear recurrence sequences; see, for example, [1, Lemma 6], [4, Lemma 9], [7, Lemma 6], [3, Lemma 6], [5, Proposition A.1], [10, Lemma 2], [11, Theorem 1]. Some, but not all, of these works are also summarised in [6, Section 5.4].

We also note some bounds on the number of zeros of general exponential polynomials modulo a high power of a prime ideal are given in [9, Theorem 2]. However, the method of [9] does not appear to extend to congruences modulo a prime ideal of large norm.

Here we first obtain a nontrivial bound on the number of zeros of reductions of quadratic exponential polynomials (1.1) over a number field K modulo integer ideals of this field. We then apply this bound to establish some arithmetic properties of such polynomials, such as lower bounds on the number of prime and integer divisors in the case when $U(x)$ is defined over $\mathbb{Z}$. We also obtain an upper bound, with a power saving on the number of zeros of quadratic exponential polynomial defined over finite fields. This appears to be the first known result of this kind.

Perhaps one of the most interesting examples of quadratic exponential polynomials (1.1) is given by $u(x^2)$, where $u(x)$ is a linear recurrence sequence. See for example, Corollary 2.4 below.

We also recall that some arithmetic properties of linear recurrence sequences at square positions have been considered in [8].

Throughout the paper, relations of the form $A = O(B)$, $A \ll B$, and $B \gg A$ are used with their usual meaning that $|A| \le cB$, where the constant c can depend on n. Furthermore, in some results the constant c can also depend on the coefficients of the exponential polynomial $U(x)$, in which case we write $A = O_U(B)$, $A \ll_U B$, and $B \gg_U A$, and similarly with other sequences.

2. Congruences with exponential polynomials

Let $\operatorname{Nm} \mathfrak{q}$ denote the norm of $\mathfrak{q}$. We state two results in this section and will prove them later in the paper.

Theorem 2.1. *Suppose* $\alpha_{i,\nu} \in \mathbb{Z}_K$, $i = 1, \dots, n$, $\nu = 0, 1, 2$ *are all relatively prime to* $\mathfrak{q}$ *and*

$$\alpha_{i,\nu}, \qquad i = 1, \dots, n, \ \nu = 1, 2,$$

are multiplicatively independent. Then

$$Q(N, \mathfrak{q}) \ll_U \frac{N}{(\log \operatorname{Nm} \mathfrak{q})^{1/(n+2)}} + N^{n/(n+1)}.$$

Obviously, for a prime ideal $\mathfrak{q} = \mathfrak{p}$, the co-primality condition of Theorem 2.1 may be weakened (since the implied constants may depend on the sequence U we can assume that $\operatorname{Nm} \mathfrak{p}$ is large enough and so the desired co-primality condition follows).

Corollary 2.2. *If* $\alpha_{i,\nu} \in \mathbb{Z}_K$, $i = 1, \dots, n$, $\nu = 0, 1, 2$, *do not vanish and*

$$\alpha_{i,\nu}, \qquad i = 1, \dots, n, \ \nu = 1, 2,$$

are multiplicatively independent, then

$$Q(N, \mathfrak{p}) \ll_U \frac{N}{(\log \operatorname{Nm} \mathfrak{p})^{1/(n+2)}} + N^{n/(n+1)}.$$

We also obtain a different bound which depends on a certain parameter which generalises the smallest multiplicative order modulo $\mathfrak{q}$ of ratios of roots of the characteristic polynomial of a linear recurrence sequence, which has been used in many previous results, see, for example Lemma 4.2 below. In fact, we can now formulate our result in the situation where the sequence is defined over a finite field $\mathbb{F}_q$ of q elements. In particular, we define

$$Q_{\mathbb{F}_q}(N) = \#\{1 \le x \le N \ : \ U(x) = 0\}.$$

Theorem 2.3. *Let* $\alpha_{i,\nu} \in \mathbb{F}_q^*$, $i = 1, \dots, n$, $\nu = 0, 1, 2$, *and let* τ *be such that no relation*

$$\prod_{i=1}^{n} \alpha_{i,1}^{k_{i,1}} = \prod_{i=1}^{n} \alpha_{i,2}^{k_{i,2}}$$

is possible with integer exponents $k_{i,\nu}$ *for which*

$$0 < \max_{i=1,\dots,n} \{|k_{i,1}|, |k_{i,2}|\} \le \tau.$$

Then

$$Q_{\mathbb{F}_q}(N) \ll N \left(N^{-1/((n+1)!-n-1)} + \tau^{-1/((n+1)!-n)} \right).$$

It is also important to note that the implied constant in Theorem 2.3 depends only on n. The condition $\alpha_{i,\nu} \in \mathbb{F}_q^*$, $i = 1, \dots, n$, that eliminates short multiplicative relations between them is generically satisfied with any $\tau < q^{1/(2n+1)-\varepsilon}$ for any fixed $\varepsilon > 0$ and sufficiently large q.

Corollary 2.4. *Let*

$$u(x) = \sum_{i=1}^{n} \alpha_i \beta_i^x$$

be a linear recurrence sequence with $\alpha_i, \beta_i \in \mathbb{F}_q^*$, $i = 1, \ldots, n$, *such that for the roots* $\beta_1, \ldots, \beta_n$ *of the characteristic polynomial we have*

$$\prod_{i=1}^{n} \beta_i^{k_i} \neq 1, \qquad 0 < \max_{i=1,\ldots,n} |k_i| \leq \tau.$$

Then

$$\#\{1 \leq x \leq N \ : \ u(x^2) = 0\} \ll_u N \left(N^{-1/((n+1)!-n-1)} + \tau^{-1/((n+1)!-n)}\right).$$

3. Prime and integer divisors of exponential polynomials

We now give some arithmetic applications of Theorem 2.1 to prime divisors of quadratic exponential polynomials (1.1) defined over $\mathbb{Z}$. We denote by $\omega(k)$ the number of distinct prime divisors of an integer $k \neq 0$. The proofs of the following theorems are also deferred.

Theorem 3.1. *Let* $\alpha_i, \beta_i, \gamma_i \in \mathbb{Z}$, $i = 1, \ldots, n$, *be such that*

$$\gcd(\alpha_1\beta_1\gamma_1, \ldots, \alpha_n\beta_n\gamma_n) = 1 \qquad \text{and} \qquad \max\{|\gamma_1|, \ldots, |\gamma_n|\} > 1.$$

Then for

$$V(x) = \sum_{i=1}^{n} \alpha_i \beta_i^x \gamma_i^{x^2}$$

we have

$$\omega\left(\prod_{x=1}^{N} \max\{1, |V(x)|\}\right) \gg_V N^{1/(n+1)}.$$

Note that the lower bound of Theorem 3.1 is of the right logarithmic order as we have the trivial upper bound $O_V(N^3/\log N)$ on the same quantity. One can also extend Theorem 3.1 to count prime ideal divisors of sequences of algebraic integers.

We now use $\tau(k)$ to denote the number of positive integer divisors of an integer $k \neq 0$. Clearly the bound of Theorem 3.1 implies that

$$\tau\left(\prod_{x=1}^{N} \max\{1, |V(x)|\}\right) \geq \exp\left(cN^{1/(n+1)}\right)$$

for some constant $c > 0$ depending on the sequence $V(x)$. Here we are able to obtain a slightly stronger bound.

Theorem 3.2. *Let* $\alpha_i, \beta_i, \gamma_i \in \mathbb{Z}$, $i = 1, \ldots, n$, *be such that*

$$\gcd(\alpha_1\beta_1\gamma_1, \ldots, \alpha_n\beta_n\gamma_n) = 1 \qquad \text{and} \qquad \max\{|\gamma_1|, \ldots, |\gamma_n|) > 1.$$

Then for

$$V(x) = \sum_{i=1}^{n} \alpha_i \beta_i^x \gamma_i^{x^2}$$

we have

$$\tau\left(\prod_{x=1}^{N}\max\{1,|V(x)|\right)\gg_V \exp\left(cN^{1/(n+1)}\log N\right)$$

for some constant $c>0$ *depending on the sequence* $V(x)$.

We remark that the argument of the proof of Theorem 3.2 can also be applied to linear recurrence sequences $u(x)$ and leads to a new result in this case as well; see (9.3) below.

4. Congruences with linear recurrence sequences

Let

$$u(x)=\sum_{h=1}^{m}\mu_h\lambda_h^x \tag{4.1}$$

be a linear recurrence sequence of order $m\ge 2$, where λ_h and μ_h, $i=1,\dots,m$, are nonzero algebraic integers in $\mathbb{Z}_K$.

We define the determinants

$$D(x_1,\dots,x_m)=\det(\lambda_h^{x_k})_{1\le h,k\le m}.$$

For a prime ideal $\mathfrak{q}$ of $\mathbb{Z}_K$, let $T(\mathfrak{q})$ be the largest nonnegative integer T with the property that

$$\mathfrak{q}\nmid\prod_{0\le x_2,\dots,x_m\le T}\max\{1,|\mathrm{Nm}\,D(0,x_2,\dots,x_m)|\},$$

where $\mathrm{Nm}\,z$ is the norm of $z\in\mathbb{Z}_K$. Clearly, if $\mathrm{Nm}\,\mathfrak{q}$ is large enough then such T always exists and we have

$$T(\mathfrak{q})\gg\frac{\log\mathrm{Nm}\,\mathfrak{q}}{\log H}, \tag{4.2}$$

where H is the largest absolute value of $\lambda_1,\dots,\lambda_m$ and their conjugates over $\mathbb{Q}$, and the implied constant depends only on m.

The parameter $T(\mathfrak{q})$ appears in the bound on the number $R(N,\mathfrak{q})$ of solutions to the congruence $u(x)\equiv 0 \pmod{\mathfrak{q}}$, $1\le x\le N$, given by [11, Lemma 1]; see also [6, Theorem 5.11].

More precisely, by [11, Lemma 1] we have:

Lemma 4.1. *Assume that* λ_h,μ_h, $h=1,\dots,m$, *are relatively prime to* $\mathfrak{q}$ *and the ratios* λ_h/λ_k, $1\le h<k\le m$, *are not roots of unity. There exists a constant* $c(m)$, *depending only on* m, *such that*

$$R(N,\mathfrak{q})\le c(m)\left(\frac{N}{T(\mathfrak{q})}+1\right).$$

We now assume that the sequence (4.1) is defined over a finite field $\mathbb{F}_q$ of q elements, that is, we have $\lambda_h,\mu_h\in\mathbb{F}_q^*$, $i=1,\dots,m$. Thus, we use $R_{\mathbb{F}_q}(N)$ to denote the number of solutions of the equation $u(x)=0$, $1\le x\le N$.

Let $\rho_{h,k}$ denote the largest multiplicative order of the ratio λ_h/λ_k, $1 \le k < h \le m$. For $m = 2$ we set, $\rho = \rho_{12}$ and for $m \ge 3$ we set

$$\rho = \max_{1 \le \ell \le m} \min_{\substack{1 \le k < h \le m \\ h \ne \ell, k \ne \ell}} \rho_{h,k}.$$

Then the following result is implied by [1, Lemma 6].

Lemma 4.2. *We have*

$$R_{\mathbb{F}_q}(N) \le (15/4)^{m-2} N \left(N^{-1/(m-1)} + \rho^{-1/(m-1)}\right).$$

Note that

$$\rho \ge \min_{1 \le k < h \le m} \rho_{h,k}$$

and this is how we use Lemma 4.2.

5. Proof of Theorem 2.1

Define $\eta = Q(N, \mathfrak{q})/N$ as the density of the solutions. We then set

$$D = \left\lceil 2(n-1)\eta^{-1} \right\rceil$$

and consider the $L+1$ intervals

$$\mathcal{I}_\nu = [\nu D + 1, (\nu+1)D], \qquad \nu = 0, \ldots, L,$$

where $L = \lfloor N/D \rfloor$.

Let J be the number of intervals $\mathcal{I}_\nu$ with at least n solutions to the congruence

$$U(x) \equiv 0 \pmod{\mathfrak{q}}, \qquad x \in \mathcal{I}_\nu.$$

Then

$$DJ + (n-1)(L+1-J) \ge Q(D(L+1), \mathfrak{q}) \ge Q(N, \mathfrak{q}).$$

Using the trivial inequality $J \ge 0$, we simplify it as

$$DJ \ge Q(N, \mathfrak{q}) - (n-1)(L+1)$$

or

$$J \ge \frac{Q(N, \mathfrak{q}) - (n-1)(L+1)}{D}. \tag{5.1}$$

Because $\eta \le 1$, we have the inequalities

$$D - 1 \le 2(n-1)\eta^{-1} \le D \le 2(n-1)\eta^{-1} + 1 \le (2n-1)\eta^{-1}. \tag{5.2}$$

In particular,

$$L \le N/D \le \frac{1}{2(n-1)}\eta N. \tag{5.3}$$

Hence, assuming that $\eta > N^{-1/3}$ as otherwise there is noting to prove, we see from (5.1) and then from (5.2) and (5.3) that

$$J \ge \frac{\eta N - (n-1)(L+1)}{(2n-1)\eta^{-1}} \ge \frac{0.5\eta N - n - 1}{(2n-1)\eta^{-1}} \ge \frac{1}{4n}\eta^2 N, \tag{5.4}$$

provided that N is large enough. In each of these J intervals with at least n solutions we choose an n-tuple of n smallest solutions, just getting J distinct n-tuples of solutions $(y+d_1, y+d_2, \dots, y+d_n)$ with $0 = d_1 < d_2 < \dots < d_n < D$.

We now choose the most frequent n-tuple, which occurs amongst these n-tuples $(y+d_1, y+d_2, \dots, y+d_n)$, which we call $(e_1, e_2, \dots, e_n)$ (where as before $e_1 = 0$). In particular,

$$U(y+e_j) \equiv 0 \pmod{\mathfrak{q}}, \qquad \nu = 1, \dots, n,$$

for at least

$$M \geq J\binom{D-1}{n-1}^{-1} \geq \frac{J(n-1)!}{(D-2)\dots(D-n)} \tag{5.5}$$

values of y in such n-tuples $(y+e_1, \dots, y+e_n)$. Since by (5.2) we have

$$(D-2)\dots(D-n) < (D-1)^{n-1} \leq (2n-2)^{n-1}\eta^{n-1},$$

combining this with (5.4) and (5.5) yields

$$M \geq \frac{(n-1)!}{2^{n+1}(n-1)^{n-1}n}\eta^{n+1}N. \tag{5.6}$$

We now see that each of the above n-tuples $(y+e_1, \dots, y+e_n)$ leads to a non-zero modulo $\mathfrak{q}$ solution

$$(z_1, \dots, z_n) = \left(\alpha_{1,0}\alpha_{1,2}^{y^2}, \dots, \alpha_{n,0}\alpha_{n,2}^{y^2}\right)$$

of the homogeneous systems of congruences

$$\sum_{i=1}^{n} z_i \beta_{i,j} \gamma_{i,\nu}^{y} \equiv 0 \pmod{\mathfrak{q}}, \qquad j = 1, \dots, n,$$

where

$$\beta_{i,j} = \alpha_{i,1}^{e_j}\alpha_{i,2}^{e_j^2} \qquad \text{and} \qquad \gamma_{i,j} = \alpha_{i,1}\alpha_{i,2}^{2e_j}.$$

Hence, we have

$$\det\left(\beta_{i,j}\gamma_{i,j}^{y}\right)_{i,j=1}^{n} \equiv 0 \pmod{\mathfrak{q}}. \tag{5.7}$$

Clearly, the determinant of the left hand side of (5.7), for $y = 1, 2, \dots$, forms a linear recurrence sequence of order $n!$. Since the $\alpha_{i,\nu}$, $i = 1, \dots, n$, $\nu = 1, 2$, are multiplicatively independent, this sequence is non-degenerate. So we can use the bound of Lemma 4.1 and note that we have

$$\log H \ll_U D \ll \eta^{-1}$$

in the bound (4.2). Hence, combining this with (5.6), we obtain

$$\eta^{n+1}N \ll_U \frac{\eta^{-1}N}{\log \operatorname{Nm}\mathfrak{q}} + 1 \tag{5.8}$$

and the desired result follows.

6. Proof of Theorem 2.3

We define $\eta = Q_{\mathbb{F}_q}(N)/N$ and proceed as in the proof of Theorem 2.1. In particular, instead of the congruence (5.7) we get a determinant equation in $\mathbb{F}_q$

$$\det\left(\beta_{i,j}\gamma_{i,j}^{y}\right)_{i,j=1}^{n} = 0$$

with similarly defined $\beta_{i,j}$ and $\gamma_{i,j}$, $i,j = 1,\dots,n$. From the definition of τ we see that we can apply Lemma 4.2 with $\rho \gg \tau/D \gg \tau\eta$, getting instead of (5.8) the inequality

$$\eta^{n+1}N \ll (15/4)^{n-2}\, N\left(N^{-1/(n!-1)} + (\tau\eta)^{-1/(n!-1)}\right).$$

7. Proof of Theorem 3.1

Let $M = \lfloor N/2 \rfloor$ and consider the product

$$W(N) = \prod_{x=M+1}^{N} |V(x)|.$$

Assume that N is large enough so that for $n \ge M$ we have $V(n) \gg \gamma^{n^2}$, where

$$\gamma = \max\{|\gamma_1|,\dots,|\gamma_n|\} > 1.$$

In particular

$$\log W(N) \gg_V N^3. \tag{7.1}$$

Let p be a prime power. Then for any integer $k \ge 1$, by Theorem 2.1 we have

$$\begin{aligned}\#\left\{x \in [M+1,N] \ :\ V(x) \equiv 0 \pmod{p^k}\right\} \\ \ll_V \frac{N}{(\log q)^{1/(n+2)}} + N^{n/(n+1)},\end{aligned} \tag{7.2}$$

where $q = \min\left\{p^k, p^{M^2}\right\}$ (note that the term p^{M^2} can be omitted if $p \nmid \gamma_1\dots\gamma_n$).

Let $\operatorname{ord}_p w$ be the p-adic order of an integer $w \ne 0$. Denoting by $\kappa_p(N)$ the largest p-adic order of $V(n)$, $M+1 \le n \le N$, and by $\mu_p(N)$ the p-adic

order of $W(N)$, we derive from (7.2)

$$\begin{aligned}\mu_p(N) &= \sum_{k=1}^{\kappa_p(N)} \#\left\{x \in [M+1, N] \ : \ V(x) \equiv 0 \pmod{p^k}\right\} \\ &\ll_V \frac{N}{(\log p)^{1/(n+2)}} \sum_{k=1}^{\kappa_p(N)} \frac{1}{\min\left\{k^{1/(n+2)}, M^{2/(n+2)}\right\}} \\ &\qquad + \kappa_p(N) N^{n/(n+1)} \\ &\ll_V \frac{N}{(\log p)^{1/(n+2)}} \sum_{k=1}^{\kappa_p(N)} \left(\frac{1}{k^{1/(n+2)}} + \frac{1}{M^{2/(n+2)}}\right) \\ &\qquad + \kappa_p(N) N^{n/(n+1)} \\ &\ll_V \frac{\kappa_p(N)^{1-1/(n+2)} N}{(\log p)^{1/(n+2)}} + \frac{\kappa_p(N) N^{n/(n+2)}}{(\log p)^{1/(n+2)}} + \kappa_p(N) N^{n/(n+1)}.\end{aligned}$$

Since the second term never dominates, we see that

$$\mu_p(N) \ll_V \frac{\kappa_p(N)^{1-1/(n+2)} N}{(\log p)^{1/(n+2)}} + \kappa_p(N) N^{n/(n+1)}. \tag{7.3}$$

Substituting the trivial bound $\kappa_p \ll_V N^2/\log p$ in (7.3), we obtain

$$\mu_p(N) \ll_V \frac{N^{3-1/(n+1)}}{\log p}. \tag{7.4}$$

Writing

$$W(N) = \prod_{p \mid W(N)} p^{\mu_p(N)}$$

and combining (7.1) and (7.4) we obtain the desired result.

8. Proof of Theorem 3.2

We define $W(N)$ and $\mu_p(N)$ as in the proof of Theorem 3.1.

We also choose some parameter $K \ge 1$ and denote $\mathcal{P}$ and $\mathcal{Q}$ be the sets of primes with

$$1 \le \mu_p(N) \le K \qquad \text{and} \qquad \mu_p(N) > K,$$

respectively. In particular,

$$\prod_{p \in \mathcal{P}} p^{\mu_p(N)} \prod_{p \in \mathcal{Q}} p^{\mu_p(N)} = W(N).$$

We consider the two cases

$$\prod_{p \in \mathcal{P}} p^{\mu_p(N)} > W(N)^{1/2} \tag{8.1}$$

and

$$\prod_{p\in\mathcal{Q}} p^{\mu_p(N)} > W(N)^{1/2} \tag{8.2}$$

separately.

Obviously, $\mu_p(N) > 0$ implies $\log p \ll_V N^2$. Hence, if (8.1) holds, then we have

$$\prod_{p\in\mathcal{P}} \log p \ge \frac{\log W(N)}{2K} \gg_V \frac{N^3}{2K},$$

which in turn yields

$$\#\mathcal{P} \gg N/K.$$

Thus

$$\tau\left(\prod_{x=1}^{N} \max\{1, |V(x)|\}\right) \ge 2^{\#\mathcal{P}} \ge \exp\left(c_1 N/K\right), \tag{8.3}$$

for some constant $c_1 > 0$, depending only on the sequence $V(x)$.

On the other hand, if (8.2) holds, then using the same argument as in the the proof of Theorem 3.1, we obtain

$$\#\mathcal{Q} \gg_V N^{1/(n+1)}.$$

Thus

$$\tau\left(\prod_{x=1}^{N} \max\{1, |V(x)|\}\right) \ge K^{\#\mathcal{Q}} \ge \exp\left(c_2 N^{1/(n+1)}\right) \tag{8.4}$$

for some constant $c_2 > 0$, depending only on the sequence $V(x)$.

Taking $K = N^{1/2}$ and combining (8.3) and (8.4), we conclude the proof.

9. Comments

It is certainly natural to ask about analogues of our results for exponential polynomials $U(x)$ of the form

$$U(x) = \sum_{i=1}^{n} \prod_{\nu=0}^{s} \alpha_{i,\nu}^{x^\nu} \tag{9.1}$$

with an integer $s \ge 2$, which we call the degree of $U(x)$.

The initial part of our argument generalises to this case without any difficulties. Namely, for integers $k \ge h \ge 0$ we set

$$c(k,h) = \binom{k}{h}.$$

Hence for any integer d we have

$$U(x+d) = \sum_{i=1}^{n} \prod_{\nu=0}^{s} \alpha_{i,\nu}^{(x+d)^\nu} = \sum_{i=1}^{n} \prod_{\nu=0}^{s} \gamma_{i,\nu}^{x^\nu},$$

where

$$\gamma_{i,\nu} = \prod_{j=\nu}^{s} \alpha_{i,j}^{c(\nu,j)d^{j-\nu}}.$$

The determinant argument applied with solutions

$$(z_1, \dots, z_n) = \left(\alpha_{1,0}\alpha_{1,s}^{y^s}, \dots, \alpha_{n,0}\alpha_{n,s}^{y^s}\right)$$

leads to a congruence with exponential polynomials of the type (9.1) with a larger value of n however of degree at most $s-1$. This, at least in principle, enables an inductive argument. However, the problem now is to control the multiplicative independence of new parameters $\gamma_{i,\nu}$, $i = 1, \dots, n$, $\nu = 1, \dots, s$.

It is also interesting to obtain analogues of our results for doubly exponential polynomials $W(x)$ of the shape

$$W(x) = \sum_{i=1}^{n} \alpha_i \beta_i^{e_i^x}. \tag{9.2}$$

The p-adic approach of [9] is likely to work for both polynomials $U(x)$ as in (9.1) and polynomials $W(x)$ as in (9.2). However, estimating the number of solutions to congruences modulo a prime or an arbitrary integer seems to be more diffficult.

On the other hand, the co-primality condition of Theorem 3.1 can be relaxed in several different ways.

Finally, we mention that the argument of the proof of Theorem 3.1 seems to be new and can also be applied to the integer linear recurrence sequences $u(x)$, giving a lower bound on the number on integer divisors of their products

$$\tau\left(\prod_{x=1}^{N} \max\{1, |u(x)|\right) \geq \exp\left(c_0 N\right), \tag{9.3}$$

with some constant $c_0 > 0$, depending on the sequence $u(x)$, which is better than the one following directly from the bound

$$\omega\left(\prod_{x=1}^{N} \max\left\{1, |u(x)|\right\}\right) \gg_u \frac{N}{\log N}$$

provided by [11, Theorem 3].

References

[1] Banks, William D.; Friedlander, John B.; Konyagin, Sergei V.; Shparlinski, Igor E. Incomplete exponential sums and Diffie–Hellman triples. *Math. Proc. Cambridge Philos. Soc.* **140** (2006), no. 2, 193–206. MR2212274, Zbl 1178.11055, doi: 10.1017/S0305004105008947. 208, 212

[2] Bugeaud, Yann; Evertse, Jan-Hendrik. S-parts of terms of integer linear recurrence sequences. *Mathematika* **63** (2017), no. 3, 840–851. MR3731307, Zbl 06843651, arXiv:1611.00485, doi: 10.1112/S0025579317000298. 207

[3] Canetti, Ran; Friedlander, John; Konyagin, Sergei; Larsen, Michael; Lieman, Daniel; Shparlinski, Igor. On the statistical properties of Diffie–Hellman distributions. *Israel J. Math.* **120** (2000), part A, 23–46. MR1815369, Zbl 0997.11066, doi: 10.1007/s11856-000-1270-1. 208

[4] Canetti, Ran; Friedlander, John; Shparlinski, Igor. On certain exponential sums and the distribution of Diffie–Hellman triples. *J. London Math. Soc.* (2) **59** (1999), no. 3, 799–812. MR1709081, Zbl 0935.11028, doi: 10.1112/S002461079900736X. 208

[5] Corvaja, Pietro; Zannier, Umberto. Finiteness of integral values for the ratio of two linear recurrences. *Invent. Math.* **149** (2002), no. 2, 431–451. MR1918678, Zbl 1026.11021, doi: 10.1007/s002220200221. 208

[6] Everest, Graham; van der Poorten, Alf; Shparlinski, Igor; Ward, Thomas. Recurrence sequences. Mathematical Surveys and Monographs, 104. *American Mathematical Society, Providence, RI*, 2003. xiv+318 pp. ISBN: 0-8218-3387-1. MR1990179, Zbl 1033.11006, doi: 10.1090/surv/104. 207, 208, 211

[7] Friedlander, John B.; Konyagin, Sergei; Shparlinski, Igor E. Some doubly exponential sums over $\mathbb{Z}_m$. *Acta Arith.* **105** (2002), no. 4, 349–370. MR1932568, Zbl 1018.11041, doi: 10.4064/aa105-4-4. 208

[8] Luca, Florian; Ward, Thomas B. An elliptic sequence is not a sampled linear recurrence sequence. *New York J. Math.* **22** (2016), 1319–1338. MR3576291, Zbl 1367.11020, arXiv:1610.08109. 208

[9] van der Poorten, Alf J.; Shparlinski, Igor E. On the number of zeros of exponential polynomials and related questions. *Bull. Austral. Math. Soc.* **46** (1992), no. 3, 401–412. MR1190343, Zbl 0753.11009, doi: 10.1017/S0004972700012065. 208, 217

[10] Shparlinski, Igor E. Prime divisors of recurrence sequences. *zv. Vyssh. Uchebn. Zaved. Mat.* 1980, no.4, 100–103. MR0580214, Zbl 437.10003. 208

[11] Shparlinski, Igor E. The number of different prime divisors of recurrence sequences. *Mat. Zametki* **42** (1987), 494–507; translated in *Math. Notes* **42** (1987), no. 3–4, 773–780). MR0917803, Zbl 0657.10007, doi: 10.1007/BF01138309. 208, 211, 217

[12] Stewart, Cameron L. On prime factors of terms of linear recurrence sequences. *Number theory and related fields*, 341–359, Springer Proc. Math. Stat., 43, *Springer, New York*, 2013. MR3081050, Zbl 1315.11011, doi: 10.1007/978-1-4614-6642-0_18. 207

(I. E. Shparlinski) Department of Pure Mathematics, University of New South Wales, Sydney, NSW 2052, Australia.
igor.shparlinski@unsw.edu.au

(U. Zannier) Scuola Normale Superiore, Piazza dei Cavalieri, 7, 56126 Pisa, Italy.
u.zannier@sns.it

This paper is available via http://nyjm.albany.edu/j/2019/25-12.html.