Acta Mathematica Academiae Paedagogicae Nyíregyháziensis
27 (2011), 211–221
www.emis.de/journals
ISSN 1786-0091

A FACTORIZATION THEOREM FOR GENERALIZED EXPONENTIAL POLYNOMIALS WITH INFINITELY MANY INTEGER ZEROS

OUAMPORN PHUKSUWAN AND VICHIAN LAOHAKOSOL

Abstract. A factorization theorem is proved for a class of generalized exponential polynomials having all but finitely many of integer zeros belong to a finite union of arithmetic progressions. This theorem extends a similar result for ordinary exponential polynomials due to H. N. Shapiro in 1959. The factorization makes apparent those factors corresponding to all zeros in such a union.

1. Introduction

There have appeared many results about different kinds of factorization of exponential polynomials, such as the ones in [9] and [8]. These factorizations aim at factoring exponential polynomials into a product of exponential polynomials of simpler forms, which resembles the factorization of natural numbers into products of primes. The kind of factorization considered in this work arises from the Skolem-Mahler-Lech theorem [11, 6, 7, 5] which states that: if an exponential polynomial has infinitely many integer zeros, then all but finitely many of such zeros form a finite union of arithmetic progressions. Based on this result, Shapiro [10], in 1959, established a factorization theorem for such exponential polynomial which makes this fact obvious. Shapiro's factorization takes the shape $F(x) = \left\{\prod_d(\eta^x - \eta^d)\right\} G(x)$, where the product is taken over all integer zeros of F belonging to a finite union of arithmetic progressions, η is a primitive root of unity, and G is an exponential polynomial with only finitely many integer zeros.

It is known that the Skolem-Mahler-Lech theorem also holds for other classes of generalized exponential polynomials, such as that in Corollary 1 in [1], with the exponent in the exponentials being a polynomial of degree greater than 1.

2010 *Mathematics Subject Classification.* 30D05, 30D15, 11L99.

Key words and phrases. generalized exponential polynomials, the Skolem-Mahler-Lech property, factorization.

Supported by the Centre of Excellence in Mathematics, the Commission on Higher Education, Thailand.

A natural question is whether there is a Shapiro-like factorization theorem for generalized exponential polynomials. The objective of this paper is to give an affirmative answer to this question.

Since the exponent in any exponential polynomial is a first degree monomial, the fact which plays a crucial role throughout Shapiro's original proof and has led to quite a number of interesting auxiliary properties. This facility is lacking in our case and makes it necessary to impose additional restrictions on the higher degree exponent. These restrictions depend on an integer parameter, denoted by t, which, when suitably chosen in many instances, is trivial. After introducing our class of generalized exponential polynomials, in the next section, we state and prove the factorization theorem.

Definition 1.1. A *pexponential polynomial* (polynomial-exponent exponential polynomial) is a function $F : \mathbb{C} \longrightarrow \mathbb{C}$ of the form

$$\begin{aligned}(1.1)\, F(x) &= \left(P_{11}(x)\rho_{11}^{Q(x)} + P_{12}(x)\rho_{12}^{Q(x)} + \cdots + P_{1n_1}(x)\rho_{1n_1}^{Q(x)}\right) A_1^{Q(x)} + \cdots \\ &\quad + \left(P_{k1}(x)\rho_{k1}^{Q(x)} + P_{k2}(x)\rho_{k2}^{Q(x)} + \cdots + P_{kn_k}(x)\rho_{kn_k}^{Q(x)}\right) A_k^{Q(x)} \\ &= \sum_{i=1}^{k} F_i(x),\end{aligned}$$

where

$$F_i(x) := A_i^{Q(x)} \sum_{j=1}^{n_i} P_{ij}(x)\rho_{ij}^{Q(x)} \quad (i = 1, \cdots, k)$$

is called the i^{th} *component*, ρ_{ij} is a δ_{ij}-th root of unity, $\delta_{ij} \in \mathbb{N}$, $\rho_{i1} = 1$, $P_{ij}(x) \in \mathbb{C}[x] \setminus \{0\}$, $Q(x) \in \mathbb{Z}[x] \setminus \mathbb{Z}$, $A_i \in \mathbb{C} \setminus \{0\}$, and $1 = |A_1| < |A_2| < \cdots < |A_k|$.

This particular shape of pexponential polynomial will be kept standard throughout the first two sections of this paper.

We pause here to mention about the origin of this definition which arises from the following observations.

(1) If a generalized exponential polynomial of the form

$$\mathcal{F}(x) = \sum_{i=1}^{n} \mathcal{A}_i^{\mathcal{Q}(x)} \mathcal{P}_i(x) \not\equiv 0$$

has infinitely many integer zeros, then there exist $i_0 \neq j_0$ such that $|\mathcal{A}_{i_0}/\mathcal{A}_{j_0}| = 1$. This is verified as follows: suppose that $|\mathcal{A}_i/\mathcal{A}_j| \neq 1$ for all $i \neq j$. Let $\mathcal{Q}(x) = c_m x^m + \cdots + c_0 \in \mathbb{Z}[x] \setminus \mathbb{Z}, c_m \neq 0$, and $Z = \{x \in \mathbb{Z} \mid \mathcal{F}(x) = 0\}$. Without loss of generality, arrange the $\mathcal{A}_i$'s so that $0 < |\mathcal{A}_1| < \cdots < |\mathcal{A}_n|$. Assume that $c_m > 0$. For $x \in Z$, we have

$$0 = \frac{\mathcal{F}(x)}{\mathcal{A}_n^{\mathcal{Q}(x)}} = \mathcal{P}_1(x)\left(\frac{\mathcal{A}_1}{\mathcal{A}_n}\right)^{\mathcal{Q}(x)} + \cdots + \mathcal{P}_{n-1}(x)\left(\frac{\mathcal{A}_{n-1}}{\mathcal{A}_n}\right)^{\mathcal{Q}(x)} + \mathcal{P}_n(x).$$

Without loss of generality, assume $\mathcal{P}_n$ does not vanish identically. The limit as $x \to +\infty$ or -∞ in Z on the right-hand side, if exists, is nonzero, which is a contradiction. The case $c_m < 0$ is similar. This leads to the grouping of components F_i in our definition of pexponential polynomials.

(2) In the case of ordinary exponential polynomial, i.e., $\deg \mathcal{Q} = 1$, Shapiro [10] showed that each unit ratio $\mathcal{A}_i/\mathcal{A}_j$ in the preceding fact is indeed a root of unity. Unfortunately, Shapiro's proof does not hold for generalized exponential polynomials with $\deg \mathcal{Q} > 1$. In another direction, Mahler in [7] used the fact that for a rational function $R(z) = \sum_{h=1}^{\infty} \mathcal{F}_h z^h$ analytic at 0, its coefficients $\mathcal{F}_h$ are exponential polynomials in h, whose exponent bases are related to the poles of $R(z)$, and these coefficients can be grouped under the pexponential polynomial form with $\deg Q = 1$. Should the coefficients $\mathcal{F}_h$ be extended to generalized exponential polynomials, the resulting function $R(z)$ is no longer a rational function and Mahler's approach cannot be carried over.

These two observations explain the restrictions about the form of our pexponential polynomials.

We now return to pexponential polynomials. A function $F(x)$ is said to have the Skolem-Mahler-Lech (or *SML*) property if whenever it has infinitely many integer zeros, there exist a positive integer Δ and a certain set $\{d_1, \ldots, d_\ell\}$ of least positive residues modulo Δ such that $F(x)$ vanishes for all integers $x \equiv d_j \pmod{\Delta}$ $(j = 1, \ldots, \ell)$ and $F(x)$ vanishes only finitely often on other integers. A pexponential polynomial having the SML-property is called *SML-pex*.

A class of examples of SML-pex's is given by taking $P_{ij}(x) \in \overline{\mathbb{Q}}[x] \setminus \{0\}$, $\log(\rho_{ij} A_i) \in \overline{\mathbb{Q}} \setminus \{0\}$, $Q(0) = 0$ and $Q'(0) \neq 0$; $\overline{\mathbb{Q}}$ denoting the algebraic closure of $\mathbb{Q}$. By Corollary 1 of [1], the corresponding $F(x)$ has the SML-property.

The integer Δ, which appears in the SML-property, is called a *period* of $F(x)$.

Clearly, any multiple of a period is also a period. Among all possible periods, the least one is called the *basic period* of $F(x)$.

For brevity, let V denote *the set of all nonzero SML-pex's with infinitely many integer zeros.* For any $F(x) \in V$ with basic period Δ, denote by $\mathcal{P}(F, \Delta)$ *the set of all least positive residues $d_1, \ldots, d_\ell$ modulo Δ mentioned in the SML-property.*

Our main result is:

Theorem 1.2. *Let $F(x)$ be a pexponential in V of the form (1.1) with basic period Δ and associated least residue set $\mathcal{P}(F,\Delta)$, let $t \in \mathbb{N}$ be such that*

$$\rho_{ij}^{t} = 1 \quad (j = 1, \ldots, n_i;\ i = 1, \ldots, k),$$

and let η be a primitive t-th root of unity. Denote by $D_1, \ldots, D_L$ $(1 \le L \le \ell)$ the partition of the set $\mathcal{P}(F,\Delta)$ with the property that if $d_i, d_j \in \mathcal{P}(F,\Delta)$ are in the same subset D_k, then $\eta^{Q(d_i)} = \eta^{Q(d_j)}$, and these last two values are not equal otherwise. Define

$$\mathcal{P}_\eta(F,\Delta) := \{D_1, \ldots, D_L\}.$$

Then $F(x)$ has a factorization of the form

$$F(x) = \left(\prod_{d \in \mathcal{P}_\eta(F,\Delta)} (\eta^{Q(x)} - \eta^{Q(d)})^{m_d} \right) G(x),$$

where $m_d \in \mathbb{N}$ and $G(x)$ is a pexponential polynomial with only finitely many integer zeros.

2. Proofs.

To prove Theorem 1.2, we need some auxiliary results. Our first lemma says roughly that infinitely many integer zeros of an SML-pex force a corresponding polynomial sum in each of its components to vanish.

Lemma 2.1. *If $F(x) \in V$, then for each $i = 1, 2, \ldots, k$, we have*

$$\sum_{j=1}^{n_i} P_{ij}(x) \rho_{ij}^{Q(d)} = 0.$$

Proof. Assume that the leading coefficient of $Q(x)$ is positive ; the other possibility is treated similarly. Substituting $x = t\Delta + d$, where $t \in \mathbb{Z}$ and $d \in \mathcal{P}(F,\Delta)$, we get

$$0 = \frac{F(t\Delta + d)}{A_k^{Q(t\Delta+d)}} = \sum_{i=1}^{k} \left(\frac{A_i}{A_k} \right)^{Q(t\Delta+d)} \sum_{j=1}^{n_i} P_{ij}(t\Delta + d) \rho_{ij}^{Q(t\Delta+d)}.$$

Then $\sum_{j=1}^{n_k} P_{kj}(t\Delta + d)\rho_{kj}^{Q(t\Delta+d)} \to 0$ $(t \to \infty)$. Taking $t = u\delta_k$, where $u \in \mathbb{Z}$, and $\delta_k = \operatorname{lcm}(\delta_{k1}, \delta_{k2}, \ldots, \delta_{kn_k})$, we obtain $\sum_{j=1}^{n_k} P_{kj}(u\delta_k\Delta + d)\rho_{kj}^{Q(d)} \to 0$ $(u \to \infty)$. Now, the polynomial $\sum_{j=1}^{n_k} P_{kj}(x)\rho_{kj}^{Q(d)} \to 0$ as $x \to \infty$ on an infinite subset of $\mathbb{Z}$ implies that it must vanish identically, and so

$$0 = F(u\delta_k\Delta + d) = \sum_{i=1}^{k-1} A_i^{Q(u\delta_k\Delta+d)} \sum_{j=1}^{n_i} P_{ij}(u\delta_k\Delta + d) \rho_{ij}^{Q(u\delta_k\Delta+d)}.$$

Repeating the steps, we have

$$0 = \frac{F(u\delta_k\Delta + d)}{A_{k-1}^{Q(u\delta_k\Delta+d)}} = \sum_{i=1}^{k-1}\left(\frac{A_i}{A_{k-1}}\right)^{Q(u\delta_k\Delta+d)} \sum_{j=1}^{n_i} P_{ij}(u\delta_k\Delta + d)\rho_{ij}^{Q(u\delta_k\Delta+d)}.$$

Thus,

$$\sum_{j=1}^{n_{k-1}} P_{(k-1)j}(u\delta_k\Delta + d)\rho_{(k-1)j}^{Q(u\delta_k\Delta+d)} \longrightarrow 0 \quad (u \longrightarrow \infty).$$

Taking $u = v\delta_{k-1}$, $v \in \mathbb{Z}$ and $\delta_{k-1} = \mathrm{lcm}(\delta_{(k-1)1}, \ldots, \delta_{(k-1)n_{k-1}})$, we have

$$\sum_{j=1}^{n_{k-1}} P_{(k-1)j}(v\delta_{k-1}\delta_k\Delta + d)\rho_{(k-1)j}^{Q(d)} \longrightarrow 0 \quad (v \longrightarrow \infty),$$

and so $\sum_{j=1}^{n_{k-1}} P_{(k-1)j}(x)\rho_{(k-1)j}^{Q(d)} = 0$. Continuing in this fashion, we get the desired result. □

The next lemma shows roughly that the result of Lemma 2.1 can be strengthened over an appropriate subset.

Lemma 2.2. *Let*

$$F(x) = \sum_{i=1}^{k} A_i^{Q(x)} \sum_{j=1}^{n_i} P_{ij}(x)\rho_{ij}^{Q(x)},$$

and let $t \in \mathbb{N}$ *be such that* $\rho_{ij}^t = 1$ *for all* $j = 1, \ldots, n_i$ *and all* $i = 1, \ldots, k$.
If $F(x) \in V$, *then*

$$\sum_{j=1}^{n_i} P_{ij}(x)\rho_{ij}^{Q(x)} = 0 \quad (i = 1, \ldots, k)$$

for all $x \in t\mathbb{Z} + d$, $d \in \mathcal{P}(F, \Delta)$.

Proof. By Lemma 2.1, $\sum_{j=1}^{n_i} P_{ij}(x)\rho_{ij}^{Q(d)} = 0$. Replacing x by $ut + d$, $u \in \mathbb{Z}$, for each $i = 1, \ldots, k$, we obtain

$$\sum_{j=1}^{n_i} P_{ij}(ut + d)\rho_{ij}^{Q(ut+d)} = 0.$$

This shows that $\sum_{j=1}^{n_i} P_{ij}(x)\rho_{ij}^{Q(x)} = 0$ for all $x \in t\mathbb{Z} + d$. □

We are now ready to prove our main result.
Proof of Theorem 1.1 By Lemma 2.2,

$$F_i(x) = A_i^{Q(x)} \sum_{j=1}^{n_i} P_{ij}(x)\rho_{ij}^{Q(x)},$$

vanishes for all $x \in t\mathbb{Z} + d$. Rewriting $F_i(x)$ as a polynomial in x with exponential coefficients, we have

$$F_i(x) = A_i^{Q(x)} \sum_m x^m (p_{1m}\rho_{i1}^{Q(x)} + \cdots + p_{n_i m}\rho_{in_i}^{Q(x)}).$$

Since the order of each $\rho_{ij} \mid t$, each ρ_{ij} is also a t-th root of unity. For each $d \in \mathcal{P}(F, \Delta)$ and $u \in \mathbb{Z}$, we get

$$\begin{aligned} 0 = F_i(ut+d) &= A_i^{Q(ut+d)} \sum_m (ut+d)^m (p_{1m}\rho_{i1}^{Q(ut+d)} + \cdots + p_{n_i m}\rho_{in_i}^{Q(ut+d)}) \\ &= A_i^{Q(ut+d)} \sum_m (ut+d)^m (p_{1m}\rho_{i1}^{Q(d)} + \cdots + p_{n_i m}\rho_{in_i}^{Q(d)}). \end{aligned}$$

This last polynomial in u vanishing identically shows that for each i,

$$p_{1m}\rho_{i1}^{Q(d)} + \cdots + p_{n_i m}\rho_{in_i}^{Q(d)} = 0.$$

Let η be a primitive t-th root of unity. Then $\rho_{ij} = \eta^{k_{ij}}$ for some $k_{ij} \in \mathbb{N}$. Thus, for each $d \in \mathcal{P}(F, \Delta)$, the element $\eta^{Q(d)}$ is a root of the polynomial $H_i(y) = p_{1m}y^{k_{i1}} + \cdots + p_{n_i m}y^{k_{in_i}}$. Thus,

$$H_i(y) = \left(\prod_{d \in \mathcal{P}_\eta(F,\Delta)} (y - \eta^{Q(d)}) \right) G_i(y),$$

where $G_i(y)$ is a polynomial. Hence

$$F_i(x) = A_i^{Q(x)} \sum_m x^m H_i(\eta^{Q(x)}) = A_i^{Q(x)} \prod_{d \in \mathcal{P}_\eta(F,\Delta)} (\eta^{Q(x)} - \eta^{Q(d)}) \sum_m x^m G_i(\eta^{Q(x)}),$$

and so

$$F(x) = \left(\prod_{d \in \mathcal{P}_\eta(F,\Delta)} (\eta^{Q(x)} - \eta^{Q(d)}) \right) \sum_i A_i^{Q(x)} \sum_m x^m G_i(\eta^{Q(x)}).$$

If $\prod_{d \in \mathcal{P}_\eta(F,\Delta)} (\eta^{Q(x)} - \eta^{Q(d)})$ exhausts all integer zeros of F belonging to each residue d_i of Δ, then $G(x) := \sum_i A_i^{Q(x)} \sum_m x^m G_i(\eta^{Q(x)})$ has only finitely many integer zeros and the factorization is complete. Otherwise, $G(x)$ has infinitely many integer zeros belonging to a subset of those of $F(x)$, which, by Δ being basic period, such zeros must belong to certain subset of residues of Δ. Since the roots of unity appearing in G are integral powers of η and $\eta^t = 1$, we can apply the same factorization steps to G. This procedure can only be repeated finitely often because $F(x)$ cannot have zeros of infinite multiplicity. The shape of the factorization factors must then be as stated. □

Corollary 2.3. *If $F(x) = \sum_{i=1}^k F_i(x) \in V$, with basic period Δ, as in the statement of Theorem 1.2, then all F_i have the term $\prod_{d \in \mathcal{P}_\eta(F,\Delta)} (\eta^{Q(x)} - \eta^{Q(d)})$ as a common factor.*

Next, we give a few examples.

Example 1. Consider, with $i=\sqrt{-1}$,

$$\begin{aligned}F(x) =& \left\{ \left(-\frac{3}{2}+\frac{\sqrt{3}}{2}i\right) + \left(-\frac{1}{2}-\frac{\sqrt{3}}{2}i\right) e^{\frac{2\pi}{3}ix^2} \right.\\ &\left. + \left(\frac{3}{2}+\frac{\sqrt{3}}{2}i\right) e^{\frac{\pi}{3}ix^2} + \left(\frac{1}{2}-\frac{\sqrt{3}}{2}i\right) e^{-\frac{\pi}{3}ix^2} \right\}\\ &+ \left\{ 1 + \left(-\frac{1}{2}-\frac{\sqrt{3}}{2}i\right) e^{\frac{\pi}{3}ix^2} + \left(-\frac{1}{2}+\frac{\sqrt{3}}{2}i\right) e^{-\frac{\pi}{3}ix^2} \right\} 3^{x^2}\\ =& \left(e^{\frac{\pi}{3}i} + (1-2e^{\frac{\pi}{3}i})e^{\frac{\pi}{3}ix^2} + (-2+e^{\frac{\pi}{3}i})e^{\frac{2\pi}{3}ix^2} + e^{\pi i x^2}\right)\left(-e^{\frac{\pi}{3}i}e^{-\frac{\pi}{3}ix^2}\right)\\ &+ \left(e^{\frac{2\pi}{3}ix^2} - e^{-\frac{\pi}{3}i}e^{\frac{\pi}{3}ix^2} - e^{\frac{\pi}{3}i}\right)\left(-e^{\frac{\pi}{3}i}e^{-\frac{\pi}{3}ix^2}\right)3^{x^2}\\ =& \left(e^{\frac{\pi}{3}ix^2}-1\right)^2\left(e^{\frac{\pi}{3}ix^2}+e^{\frac{\pi}{3}i}\right)\left(-e^{\frac{\pi}{3}i}e^{-\frac{\pi}{3}ix^2}\right)\\ &+ \left(e^{\frac{\pi}{3}ix^2}-1\right)\left(e^{\frac{\pi}{3}ix^2}+e^{\frac{\pi}{3}i}\right)\left(-e^{\frac{\pi}{3}i}e^{-\frac{\pi}{3}ix^2}\right)3^{x^2}\\ =& \left(e^{\frac{\pi}{3}ix^2}-1\right)\left(e^{\frac{\pi}{3}ix^2}+e^{\frac{\pi}{3}i}\right)\left(-e^{\frac{\pi}{3}i}e^{-\frac{\pi}{3}ix^2}\right)\left(3^{x^2}+e^{\frac{\pi}{3}ix^2}-1\right).\end{aligned}$$

Here,

$$Q(x)=x^2,\ A_1=1, A_2=3,$$

$$\rho_{11}=1,\ \rho_{12}=e^{\frac{2\pi}{3}i},\ \rho_{13}=e^{\frac{\pi}{3}i},\ \rho_{14}=e^{-\frac{\pi}{3}i},\ \rho_{21}=1,\ \rho_{22}=e^{\frac{\pi}{3}i},\ \rho_{23}=e^{-\frac{\pi}{3}i},$$

$$P_{11}(x)=-\frac{3}{2}+\frac{\sqrt{3}}{2}i,\ P_{12}(x)=-\frac{1}{2}-\frac{\sqrt{3}}{2}i,\ P_{13}(x)=\frac{3}{2}+\frac{\sqrt{3}}{2}i,\ P_{14}(x)=\frac{1}{2}-\frac{\sqrt{3}}{2}i,$$

$$P_{21}=1,\ P_{22}(x)=-\frac{1}{2}-\frac{\sqrt{3}}{2}i,\ P_{23}(x)=-\frac{1}{2}+\frac{\sqrt{3}}{2}i.$$

Solving for integer zeros of $F(x)$, we get $x\equiv 0,2,4 \mod 6$. Thus, $\Delta=6, d_1=0, d_2=2$, and $d_3=4$. Here, we choose $t=6$ to fulfill $\rho_{ij}^t=1$ for all i,j, and so $\eta=e^{i\pi/3}$ is a primitive 6-th root of unity. It is easy to check that $\eta^{Q(d_2)}=e^{\frac{\pi}{3}i2^2}=e^{\frac{\pi}{3}i4^2}=\eta^{Q(d_3)}$. The factorization stated in Theorem 1.2 is

$$F(x)=\left(e^{\frac{\pi}{3}ix^2}-1\right)\left(e^{\frac{\pi}{3}ix^2}+e^{\frac{\pi}{3}i}\right)\ e^{\frac{4\pi}{3}i}e^{-\frac{\pi}{3}ix^2}(3^{x^2}+e^{\frac{\pi}{3}ix^2}-1),$$

where $m_{d_1}=m_{d_2}=1$ and $G(x)=e^{\frac{4\pi}{3}i}e^{-\frac{\pi}{3}ix^2}(3^{x^2}+e^{\frac{\pi}{3}ix^2}-1)$.

Example 2. Let, with $i=\sqrt{-1}$,

$$F(x)=1-e^{\frac{\pi}{2}ix^2}-e^{\frac{\pi}{3}ix^2}+e^{\frac{5\pi}{6}ix^2}=\left(e^{\frac{\pi}{3}ix^2}-1\right)\left(e^{\frac{\pi}{2}ix^2}-1\right).$$

Here,

$$Q(x)=x^2,\ A=1,\ \rho_1=1,\ \rho_2=e^{\frac{\pi}{2}i},\ \rho_3=e^{\frac{\pi}{3}i},\ \rho_4=e^{\frac{5\pi}{6}i},$$

and

$$P_1(x) = P_2(x) = P_3(x) = P_4(x) = 1.$$

Direct computations show that

$$\Delta = 6,\ d_1 = 0,\ d_2 = 2,\ d_3 = 4.$$

We choose $t = 12$, and so $\eta = e^{\frac{\pi}{6}i}$ is a primitive 12-th root of unity. Since $\eta^{Q(d_2)} = e^{\frac{\pi}{6}i2^2} = e^{\frac{\pi}{6}i4^2} = \eta^{Q(d_3)}$, Theorem 1.2 yields

$$F(x) = \left(e^{\frac{\pi}{6}ix^2} - 1\right)^2 \left(e^{\frac{\pi}{6}ix^2} - e^{\frac{2\pi}{3}i}\right)^2 \left(e^{\frac{\pi}{6}ix^2} + 1\right),$$

where $m_{d_1} = m_{d_2} = 2$ and $G(x) = e^{i\pi x^2/6} + 1$.

3. An improved theorem

The results and details in this section have been provided to us by the anonymous referee whose generosity is most appreciated. The class of generalized exponential polynomials, which can be factored as in Theorem 1.2, can be substantially enlarged through the use of p-adic analysis. We have decided to put this discussion in a new section because the method involved differs markedly from our earlier simple analysis. The much improved result is:

Theorem 3.1. *Let F be a non-trivial generalized exponential polynomial of the form*

$$F(x) = \sum_{i=1}^{k} P_i(x) A_i^{Q(x)}, \tag{3.1}$$

where the A_i's are distinct elements of $\mathbb{C} \setminus \{0\}$, $P_i(x) \in \mathbb{C}[x] \setminus \{0\}$ and $Q(x) \in \mathbb{Z}[x] \setminus \mathbb{Z}$. If F has infinitely many integer zeros, then there exist $T \in \mathbb{N}$ and a subset $E \subseteq \{0, 1, \ldots, T-1\}$ such that

$$F(x) = \left(\prod_{r\in E} \left(\eta^{Q(x)} - \eta^{Q(r)}\right)^{m_r}\right) G(x),$$

where η is a primitive T^{th} root of unity, $m_r \in \mathbb{N}$, and G is a generalized exponential polynomial of the same form (3.1) *but with finitely many integer zeros.*

To prove Theorem 3.1, we need:

Lemma 3.2. *Let F be as in* (3.1). *If F has infinitely many integer zeros, then for each $i \in \{1, \ldots, k\}$, there exists $j \neq i$ such that $A_i A_j^{-1}$ is a root of unity, and there exists $T \in \mathbb{N}$ such that for each $r \in \{0, \ldots, T-1\}$, we have either $F(xT + r) = 0$ for all $x \in \mathbb{Z}$, or there are only finitely many $x \in \mathbb{Z}$ for which $F(xT + r) = 0$.*

Proof. Let C be the set consisting of all the relevant coefficients and exponents in F. Namely,

$$C := \{A_i \ (i=1,\ldots,k), \text{ the nonzero coefficients of } Q \text{ and of } P_i \ (i=1,\ldots,k)\}.$$

By Cassels' embedding theorem [3, 2] (see also [4]), we can embed K into a $\mathbb{Q}_p$, the field of $p-$adic numbers, with the property that all elements of C become $p-$adic units. Thus, A_i^{p-1} is congruent to 1 modulo p in $\mathbb{Z}_p$, the ring of $p-$adic integers. Consequently, the function $y \mapsto \left(A_i^{p-1}\right)^y$ is defined and analytic in the closed unit disk of $\mathbb{C}_p$, the completion of the algebraic closure of $\mathbb{Q}_p$. For each $r \in \{0,\ldots,p-2\}$, since

$$Q(x(p-1)+r) = (p-1)S_r(x) + Q(r)$$

with $S_r \in \mathbb{Z}[x]$, the function

$$x \in \mathbb{C}_p \longmapsto A_i^{Q((p-1)x+r)} = \left(A_i^{p-1}\right)^{S_r(x)} A_i^{Q(r)}$$

is analytic in the closed unit disk of $\mathbb{C}_p$, and so is the function $F(x(p-1)+r)$. Now for each $r \in \{0,\ldots,p-2\}$, if the function $F(x(p-1)+r)$ is zero, then $F(x(p-1)+r) = 0$ for all $x \in \mathbb{Z}$, and if the function $F(x(p-1)+r)$ is not zero, then this function has only a finite number of zeros in the closed unit disk of $\mathbb{C}_p$, and $F(x(p-1)+r)$ has only a finite number of zeros in $\mathbb{Z}$.

Suppose that for some $r \in \{0,\ldots,p-2\}$, the function $F(x(p-1)+r)$ is the zero function. Let $B_1,\ldots,B_t$ be the distinct elements of the set

$$\left\{A_i^{p-1};\ i=1,\ldots,k\right\}.$$

The function $F(x(p-1)+r)$ takes the form $\sum_{i=1}^t Q_i(x)B_i^{S_r(x)}$, where the Q_i's are polynomials.

We claim now that all of the Q_i's are zero.

We prove this by induction on t. The case $t=1$ is trivial. Suppose the result is true for $t-1$. Assume that $B_t \not\equiv 0$, for otherwise we are done by induction. Divide through by $B_t^{S_r(x)}$, and then differentiate the expression sufficiently many times until the term Q_t disappears. Note that if "log" denotes the $p-$adic logarithm, then $\log(B_iB_t^{-1})$ is not zero, as $B = B_iB_t^{-1}$ is congruent to 1 mod p but not equal to 1, and if $R(x) = H(x)B^{Q(x)}$ with a nonzero polynomial H, then the derivative of R is of the form $H^*(x)B^{Q(x)}$ with $\deg H^* \geq \deg H$. The resulting expression, after a sufficient number of differentiations, is thus of the same form with one fewer term and the induction hypothesis yields the desired conclusion.

This shows that if there exists $r \in \{0,\ldots,p-2\}$ such that $F(x(p-1)+r)$ has infinitely many integer zeros, then for each $i \in \{1,\ldots,k\}$, since $P_i(x) \in \mathbb{C}[x]\setminus\{0\}$, there exists j such that $A_i^{p-1} = A_j^{p-1}$, i.e., $A_iA_j^{-1}$ is a root of unity, and so there exists $T \in \mathbb{N}$, which can of course be $p-1$ or the least common multiple of the orders of these roots of unity, with the property prescribed in the statement of the Lemma. $\square$

We proceed now to prove Theorem 3.1.

Proof of Theorem 3.1 By Lemma 3.2, denote by $C_1, \dots, C_m$, all those A_i $(i = 1, \dots, k)$ having the property that none of the $C_k C_\ell^{-1}$ is a root of unity for $k \neq \ell$, and for each i, write

$$A_i = C_{k_i} \eta^{s_i} \quad (i = 1, \dots, k),$$

where η is a primitive T-th root of unity, and $s_i \in \mathbb{N}$. Thus,

$$F(x) = \sum_{k=1}^{m} C_k^{Q(x)} \sum_{i=1}^{n_k} H_i(x) \eta^{s_{i,k} Q(x)},$$

where $n_k \in \mathbb{N}$, H_i's are polynomials, and $s_{i,k} \in \mathbb{N}$.

If $r \in \{0, \dots, T-1\}$ is such that $F(xT+r)$ has infinitely many integer zeros, then so does

$$\sum_{k=1}^{m} C_k^{Q(xT+r)} \sum_{i=1}^{n_k} H_i(xT+r) \eta^{s_{i,k} Q(r)} = \sum_{k=1}^{m} C_k^{Q(xT+r)} \sum_{i=1}^{n_k} H_i(xT+r) \eta^{s_{i,k} Q(xT+r)}.$$

By Lemma 3.2 again, as $C_k C_l^{-1}$ are not roots of unity for $k \neq l$, by the same arguments as in the proof of the claim in the middle of the proof of Lemma 3.2, all the coefficients $\sum_{i=1}^{n_k} H_i(xT+r) \eta^{s_{i,k} Q(r)}$ are zero, implying that $\sum_{i=1}^{n_k} H_i(x) \eta^{s_{i,k} Q(r)}$ is also zero. Thus, F can be written as

$$\begin{aligned} F(x) &= \sum_{k=1}^{m} C_k^{Q(x)} \left(\sum_{i=1}^{n_k} H_i(x) \eta^{s_{i,k} Q(x)} - \sum_{i=1}^{n_k} H_i(x) \eta^{s_{i,k} Q(r)} \right) \\ &= \sum_{k=1}^{m} C_k^{Q(x)} \sum_{i=1}^{n_k} H_i(x) \left(\eta^{s_{i,k} Q(x)} - \eta^{s_{i,k} Q(r)} \right). \end{aligned}$$

Since $\eta^{Q(x)} - \eta^{Q(r)}$ divides each factor $\eta^{s_{i,k} Q(x)} - \eta^{s_{i,k} Q(r)}$, we get

$$F(x) = \left(\eta^{Q(x)} - \eta^{Q(r)} \right) G(x),$$

where G is a generalized exponential polynomial of the same form

$$\sum_{k=1}^{m} C_k^{Q(x)} \sum_{i=1}^{n_k} \mathcal{H}_i(x) \eta^{m_{i,k} Q(x)}.$$

The desired factorization follows in a finite number of similar repeated operations. $\square$

References

[1] J.-P. Bézivin and V. Laohakosol. On the theorem of Skolem-Mahler-Lech. *Exposition. Math.*, 9(1):89–96, 1991.

[2] J. W. S. Cassels. Addendum: "An embedding theorem for fields" (Bull. Austral. Math. Soc. **14** (1976), no. 2, 193–198). *Bull. Austral. Math. Soc.*, 14(3):479–480, 1976.

[3] J. W. S. Cassels. An embedding theorem for fields. *Bull. Austral. Math. Soc.*, 14(2):193–198, 1976.

[4] J. W. S. Cassels. *Local fields*, volume 3 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1986.

[5] C. Lech. A note on recurring series. *Ark. Mat.*, 2:417–421, 1953.

[6] K. Mahler. Eine arithmetische Eigenschaft der Taylor-Koeffizienten rationaler Funktionen. *Proc. Akad. Wet. Amsterdam*, 38:50–60, 1935.

[7] K. Mahler. On the Taylor coefficients of rational functions. *Proc. Cambridge Philos. Soc.*, 52:39–48, 1956.

[8] O. Phuksuwan, P. Udomkavanich, and V. Laohakosol. An analysis of Ritt's factorization for exponential sums. *East-West J. Math.*, (Special Vol.):61–72, 2004.

[9] J. F. Ritt. A factorization theory for functions $\sum_{i=1}^{n} a_i e^{\alpha_i x}$. *Trans. Amer. Math. Soc.*, 29(3):584–596, 1927.

[10] H. N. Shapiro. On a theorem concerning exponential polynomials. *Comm. Pure Appl. Math.*, 12:487–500, 1959.

[11] T. Skolem. Ein Verfahren zur Behandlung gewisser exponentialer Gleichungen und diophantischer Gleichungen. 8. Skand. Mat. Kongr., Stockhohn, 163–188, 1934.

Received January 28, 2011.

Ouamporn Phuksuwan,
Department of Mathematics and Computer Science,
Faculty of Science,
Chulalongkorn University,
Bangkok 10330,
Thailand
E-mail address: `ouamporn.p@chula.ac.th`

Vichian Laohakosol,
Department of Mathematics,
Kasetsart University,
Bangkok 10900,
and
Centre of Excellence in Mathematics,
Si Ayutthaya Road,
Bangkok 10400,
Thailand
E-mail address: `fscivil@ku.ac.th`