Aequat. Math.

https://doi.org/10.1007/s00010-023-00996-5

Aequationes Mathematicae

The Artin-Hasse series and Laguerre polynomials modulo a prime

Marina Avitabile and Sandro Mattarei

Abstract. For an odd prime p, let $\mathrm{E}_p(X) = \sum_{n=0}^{\infty} a_n X^n \in \mathbb{F}_p[[X]]$ denote the reduction modulo p of the Artin-Hasse exponential series. It is known that there exists a series $G(X^p) \in \mathbb{F}_p[[X]]$, such that $L_{p-1}^{(-T(X))}(X) = \mathrm{E}_p(X) \cdot G(X^p)$, where $T(X) = \sum_{i=1}^{\infty} X^{p^i}$ and $L_{p-1}^{(\alpha)}(X)$ denotes the (generalized) Laguerre polynomial of degree $p-1$. We prove that $G(X^p) = \sum_{n=0}^{\infty}(-1)^n a_{np} X^{np}$, and show that it satisfies $G(X^p)\,G(-X^p)\,T(X) = X^p$.

Mathematics Subject Classification. Primary 33E50, Secondary 33C45.

Keywords. Artin-Hasse series, Laguerre polynomials.

1. Introduction

Let p be a prime. The Artin-Hasse exponential series is the formal power series in $\mathbb{Q}[[X]]$ defined as

$$\mathrm{AH}(X) = \exp\left(\sum_{i=0}^{\infty} X^{p^i}/p^i\right) = \prod_{i=0}^{\infty} \exp\left(X^{p^i}/p^i\right).$$

As an immediate application of the Dieudonné-Dwork criterion, its coefficients are p-integral, hence they can be evaluated modulo p. Let $\mathrm{E}_p(X) = \sum a_n X^n$ denote the reduction modulo p of the Artin-Hasse exponential series, hence viewed as a series in $\mathbb{F}_p[[X]]$.

The series $\mathrm{E}_p(X)$ satisfies a weak version of the functional equation $\exp(X)\exp(Y) = \exp(X+Y)$ of the classical exponential series $\exp(X) = \sum X^k/k!$ in characteristic zero. In fact, it was shown in [7, Theorem 2.2] that each term of the series $(\mathrm{E}_p(X+Y))^{-1}\,\mathrm{E}_p(X)\,\mathrm{E}_p(Y)$ has degree a multiple of p. This weak functional equation satisfied by $\mathrm{E}_p(X)$ is the crucial property needed for a *grading switching* technique developed in [7], whose goal is producing a new grading of a non-associative algebra A in characteristic p from

Published online: 10 October 2023

a given grading. Roughly speaking, the new grading of A is obtained by applying $\mathrm{E}_p(D)$ to each homogeneous components of the given grading, where D is a nilpotent derivation of A satisfying a certain compatibility condition with the grading. In full generality, that is for arbitrary derivations, the grading switching was developed in [3]. The *toral switching* (see [10], [5] and [9]), a fundamental tool in the classification theory of simple modular Lie algebras, can be recovered as a special case of it.

In this Introduction we limit ourselves to a brief survey of the definitions and the results which are essential for the purposes of this paper, referring the reader to Sect. 2 for further details, and the interested reader to [3] and [2] for full details. In the general case of the grading switching, the role of the Artin-Hasse exponential is played by the (generalized) Laguerre polynomials of degree $p-1$,

$$L_{p-1}^{(\alpha)}(X) = \sum_{k=0}^{p-1} \binom{\alpha-1}{p-1-k} \frac{(-X)^k}{k!}, \tag{1}$$

regarded as polynomials in $\mathbb{F}_p[\alpha, X]$. These polynomials satisfy a congruence which can be interpreted as a further generalization of the weak functional equation satisfied by $\mathrm{E}_p(X)$. The main result of [8] then implies that the power series

$$S(X) = L_{p-1}^{(-\sum_{i=1}^{\infty} X^{p^i})}(X),$$

in $1 + X\mathbb{F}_p[[X]]$, satisfies $S(X) = E_p(X) \cdot G(X^p)$ for some series $G(X) \in 1 + X\mathbb{F}_p[[X]]$. Our main result is to determine the coefficients of the series $G(X)$ in terms of those of $\mathrm{E}_p(X)$. We separately deal with the case $p = 2$ in Remark 7. When p is an odd prime we have the following.

Theorem 1. *Let p be an odd prime, and let $\mathrm{E}_p(X) = \sum_{n=0}^{\infty} a_n X^n$ in $\mathbb{F}_p[[X]]$ be the reduction modulo p of the Artin-Hasse exponential series. Then*

$$L_{p-1}^{(-\sum_{i=1}^{\infty} X^{p^i})}(X) = \mathrm{E}_p(X) \cdot \sum_{n=0}^{\infty} (-1)^n a_{np} X^{np}, \tag{2}$$

and

$$L_{p-1}^{(-\sum_{i=1}^{\infty} X^{p^i})}(X) \cdot \left(\sum_{i=1}^{\infty} X^{p^i} \right) \cdot \sum_{n=0}^{\infty} a_{np} X^{np} = X^p \, \mathrm{E}_p(X) \tag{3}$$

in $\mathbb{F}_p[[X]]$.

As an immediate consequence of Theorem 1 we have the following result.

Proposition 2. *Let p be an odd prime and $\mathrm{E}_p(X) = \sum_{i=0}^{\infty} a_i X^i$ in $\mathbb{F}_p[[X]]$ the reduction modulo p of the Artin-Hasse exponential series. Then in $\mathbb{F}_p[[X]]$ we have the identity*

$$\sum_{s=0}^{\infty} a_{sp} X^{sp} \cdot \sum_{r=0}^{\infty} a_{rp} (-X)^{rp} \cdot \sum_{i=1}^{\infty} X^{p^i} = X^p. \tag{4}$$

Proposition 2 can equivalently be phrased in the following form involving the series $\sum_{p|k} X^k/k!$ in place of the Artin-Hasse series.

Proposition 3. *For any odd prime p, in $\mathbb{Q}[[X]]$ we have*

$$\sum_{s=0}^{\infty} \frac{X^{sp}}{(sp)!} \cdot \sum_{r=0}^{\infty} \frac{(-X)^{rp}}{(rp)!} \cdot \sum_{i=1}^{\infty} X^{p^i} \equiv X^p \pmod{p}.$$

Despite its appearance, the left-hand side of the congruence of Proposition 3 has p-integral coefficients, which justifies viewing it modulo p. This variant does not seem to offer any more direct proof than deducing it from Proposition 2, which we will do in Sect. 3.

As a final application of Theorem 1, we use properties of the Laguerre polynomials to produce explicit expressions for the coefficients a_n, with $0 \leq n < p^2$, in terms of coefficients in the same range but with n multiple of p. We denote by $\left[\begin{smallmatrix} n \\ i \end{smallmatrix}\right]$ the (unsigned) Stirling numbers of the first kind.

Proposition 4. *For $0 \leq k < p$ and $0 \leq r < p$ we have*

$$a_{rp+k} = (-1)^{k+1} \sum_{j=0}^{r} \begin{bmatrix} p-k \\ j+1 \end{bmatrix} c_{(r-j)p},$$

where $c_{jp} = a_{jp}$ for $0 \leq j < p-1$ and $c_{(p-1)p} = a_{(p-1)p} + 1$.

We present proofs of our results in Sect. 3.

2. Preliminaries

Let $\mathbb{Z}_p$ denote the ring of p-adic integers, where p is any prime, and write

$$\mathrm{AH}(X) = \sum_{n=0}^{\infty} u_n X^n \in \mathbb{Z}_p[[X]]. \tag{5}$$

The coefficients u_n satisfy the *recursive formula* (see [6, Lemma 1])

$$u_n = \frac{1}{n} \sum_{i=0}^{\infty} u_{n-p^i}, \tag{6}$$

where $u_0 = 1$ and we naturally read $u_m = 0$ for $m < 0$, which easily follows from differentiating Eq. (5).

Our interest lies exclusively in prime characteristic p. Denote by $\mathrm{E}_p(X) = \sum a_n X^n \in \mathbb{F}_p[[X]]$ the reduction modulo p of the Artin-Hasse exponential series, hence $a_n \equiv u_n$ modulo p. As mentioned in the Introduction, $\mathrm{E}_p(X)$ satisfies a functional equation which is a weak version of the fundamental equation $\exp(X)\exp(Y) = \exp(X+Y)$ for the classical exponential series $\exp(X) = \sum X^k/k!$ in characteristic zero. Namely, as shown in the proof of [7, Theorem 2.2], we have

$$\mathrm{E}_p(X)\,\mathrm{E}_p(Y) = \mathrm{E}_p(X+Y)\left(1 + \sum_{i,j} a_{i,j} X^i Y^j\right) \tag{7}$$

in $\mathbb{F}_p[[X,Y]$, for some coefficients $a_{i,j} \in \mathbb{F}_p$ which vanish unless $p \mid i+j$. The functional Eq. (7) actually characterizes the series $\mathrm{E}_p(X)$ in $\mathbb{F}_p[[X]]$, up to some natural variations. Precisely, we quote from [8] the following

Theorem 5. ([8]) *For a series $S(X) \in 1 + X\mathbb{F}_p[[X]]$, the series*

$$(S(X+Y))^{-1}\, S(X)\, S(Y) \in \mathbb{F}_p[[X,Y]]$$

has only terms of total degree a multiple of p if and only if

$$S(X) = \mathrm{E}_p(cX) \cdot G(X^p),$$

for some $c \in \mathbb{F}_p$ and $G(X) \in 1 + X\mathbb{F}_p[[X]]$.

The classical (generalized) Laguerre polynomial of degree $n \geq 0$ is defined as

$$L_n^{(\alpha)}(X) = \sum_{k=0}^{n} \binom{\alpha+n}{n-k} \frac{(-X)^k}{k!},$$

where α is a parameter, usually in the complex field. However, we may also view $L_n^{(\alpha)}(X)$ as a polynomial with rational coefficients in the two indeterminates α and X, hence in the polynomial ring $\mathbb{Q}[\alpha, X]$. We are only interested in the Laguerre polynomials of degree $n = p-1$. Their coefficients are p-integral, and hence can be evaluated modulo p. In particular, $L_{p-1}^{(\alpha)}(X)$ will be viewed as a polynomial in $\mathbb{F}_p[\alpha, x]$, and as such will be given by Eq. (1). Note that, for $\alpha = 0$, $L_{p-1}^{(0)}(X)$ equals the *truncated exponential* $\mathrm{E}(X) = \sum_{k=0}^{p-1} X^k/k!$, which in turns is congruent to $\mathrm{E}_p(X)$ modulo X^p.

The Laguerre polynomials $L_{p-1}^{(\alpha)}(X)$ satisfy a congruence which can be interpreted as a further generalization of Eq. (7). Indeed, it follows from [3, Proposition 2] (but see also [4, Theorem 1] for a streamlined statement) that there exist rational expressions $c_i(\alpha,\beta) \in \mathbb{F}_p(\alpha,\beta)$ such that

$$L_{p-1}^{(\alpha)}(X) L_{p-1}^{(\beta)}(Y) \equiv L_{p-1}^{(\alpha+\beta)}(X+Y)\left(c_0(\alpha,\beta) + \sum_{i=1}^{p-1} c_i(\alpha,\beta) X^i Y^{p-i}\right), \tag{8}$$

in $\mathbb{F}_p(\alpha,\beta)[X,Y]$, modulo the ideal generated by $X^p-(\alpha^p-\alpha)$ and $Y^p-(\beta^p-\beta)$. This congruence actually characterizes the polynomials $L_{p-1}^{(\alpha)}(X)$ among those in $\mathbb{F}_p[\alpha][X]$, up to some natural variations, as proved in [4, Theorem 3].

In the rest of the paper we let $S(X)$ denote the power series in $1+X\mathbb{F}_p[[X]]$ defined as

$$S(X)=L_{p-1}^{(-\sum_{i=1}^{\infty}X^{p^i})}(X).$$

According to [2, Proposition 6] to which we refer for details, Eq. (8) implies that $(S(X+Y))^{-1}S(X)S(Y)$ has only terms of degree divisible by p. According to Theorem 5, since $S(X)\equiv L_{p-1}^{(0)}(X)=\mathrm{E}(X)\equiv \mathrm{E}_p(X)$ modulo X^p, we have

$$S(X)=\mathrm{E}_p(X)\cdot G(X^p) \tag{9}$$

for some $G(X)$ in $1+X\mathbb{F}_p[[X]]$. Equivalently, we have

$$S(X)\cdot F(X^p)=\mathrm{E}_p(X), \tag{10}$$

for some $F(X)=1/G(X)$ in $1+X\mathbb{F}_p[[X]]$. Our Theorem 1 produces explicit expressions for $G(X^p)$ and $F(X^p)$.

3. Proofs

In this section we prove Theorem 1, Proposition 2 and Proposition 4. We will need the following special instance of Eq. (8).

Lemma 6. ([1, Lemma 10]) *In the polynomial ring $\mathbb{F}_p[\alpha,X]$ we have*

$$L_{p-1}^{(\alpha)}(X)\cdot L_{p-1}^{(-\alpha)}(-X)\equiv 1-\alpha^{p-1}\pmod{X^p-(\alpha^p-\alpha)}.$$

Note that $L_{p-1}^{(\alpha)}(0)=\binom{\alpha-1}{p-1}=1-\alpha^{p-1}=L_{p-1}^{(-\alpha)}(0)$.

Proof of Theorem 1. From Eq. (9) and the fact that $\mathrm{E}_p(X)\,\mathrm{E}_p(-X)=1$ (for p odd) we deduce

$$T(X)\cdot S(X)\cdot S(-X)\cdot \mathrm{E}_p(-X)=T(X)\cdot S(-X)\cdot G(X^p),$$

where $T(X)=\sum_{i=1}^{\infty}X^{p^i}$. To fix notation we set $G(X^p)=\sum_{n=0}^{\infty}b_{np}X^{np}$. Setting $\alpha=-T(X)$ in Lemma 6 we find $S(X)\cdot S(-X)=1-T(X)^{p-1}$. In more formal terms we have applied to the congruence the ring homomorphism of $\mathbb{F}_p[\alpha,X]$ to $\mathbb{F}_p[[X]]$ which maps α to $-T(X)$, noting that the modulus $X-(\alpha^p-\alpha)$ belongs to its kernel. Consequently, $T(X)\cdot S(X)\cdot S(-X)=X^p$, because $T(X)-T(X)^p=X^p$, and hence

$$X^p\cdot\sum_{n=0}^{\infty}(-1)^n a_nX^n=T(X)\cdot S(-X)\cdot\sum_{n=0}^{\infty}b_{np}X^{np}.$$

Now we are only interested in the terms of this equation where the exponent of X is a multiple of p. In the case of $S(-X) = L_{p-1}^{(T(X))}(-X)$ the collection of such terms equals

$$\binom{T(X)-1}{p-1} = 1 - T(X)^{p-1}$$

in $\mathbb{F}_p(X)$. Because $T(X) - T(X)^p = X^p$ we conclude

$$X^p \sum_{n=0}^{\infty} (-1)^n a_{np} X^{np} = X^p \sum_{n=0}^{\infty} b_{np} X^{np},$$

which is equivalent to Eq. (2).

To prove Eq. (3) we proceed in a similar way, starting from $S(X) \cdot F(X^p) = \mathrm{E}_p(X)$ in $\mathbb{F}_p[[X]]$. Setting $F(X^p) = \sum_{n=0}^{\infty} c_{np} X^{np}$ we have

$$T(X) \cdot S(X) \cdot \sum_{n=0}^{\infty} c_{np} X^{np} = T(X) \cdot \sum_{n=0}^{\infty} a_n X^n.$$

Restricting to powers of X with exponent a multiple of p in each side we obtain

$$X^p \cdot \sum_{n=0}^{\infty} c_{np} X^{np} = T(X) \cdot \sum_{n=0}^{\infty} a_{np} X^{np},$$

which is equivalent to Eq. (3). □

Remark 7. Although Theorem 1 does not extend to $p = 2$ as stated, a replacement for Eq. (3) is easily found directly. Indeed, $L_1^{(\alpha)}(X) = 1 + \alpha + X$ and the recursive formula Eq. (6) implies $a_{2n} = a_{2n+1} + \sum_{i=1}^{\infty} a_{2n+1-2^i}$ for every integer n, where $a_n = 0$ for $n < 0$. Hence,

$$\begin{aligned}
\mathrm{E}_2(X) &= \sum_{n=0}^{\infty} a_{2n} X^{2n} + \sum_{n=0}^{\infty} a_{2n+1} X^{2n+1} \\
&= (1+X) \sum_{n=0}^{\infty} a_{2n+1} X^{2n} + \sum_{n=0}^{\infty} \left(\sum_{i=1}^{\infty} a_{2n+1-2^i} \right) X^{2n} \\
&= (1 + X + \sum_{i=1}^{\infty} X^{2^i}) \sum_{n=0}^{\infty} a_{2n+1} X^{2n} = S(X) \sum_{n=0}^{\infty} a_{2n+1} X^{2n}.
\end{aligned}$$

Thus, when $p = 2$ Eq. (10) holds with $F(X^2) = \sum_{n=0}^{\infty} a_{2n+1} X^{2n}$.

Theorem 1 immediately implies Proposition 2.

Proof of Proposition2. Our goal can be restated as

$$G(X^p)\, G(-X^p)\, T(X) = X^p.$$

Now $G(X^p)\,G(-X^p) = S(X)\,S(-X) = 1 - T(X)^{p-1}$, as we deduced from Lemma 6 at the beginning of the proof of Theorem 1. The conclusion follows because $G(X^p) = \sum_{r=0}^{\infty}(-1)^r a_{rp} X^{rp}$ according to Theorem 1. □

Deducing Proposition 3 from Proposition 2 requires the technique of series multisection.

Proof of Proposition 3. In terms of $e_p(X) = \sum_{p|k} X^k/k!$, our goal becomes the congruence

$$e_p(X)\,e_p(-X)\sum_{i=1}^{\infty} X^{p^i} \equiv X^p \pmod p$$

from the equation

$$G(X^p)\,G(-X^p)\,T(X) = X^p$$

in $\mathbb{F}_p[[X]]$. We have $e_p(X) = (1/p)\sum_{\omega^p=1}\exp(\omega X)$, where the sum is over all complex pth roots of unity ω.

Because of the equation

$$\mathrm{AH}(X) = \prod_{i=0}^{\infty}\exp\left(X^{p^i}/p^i\right) = \exp(X)\,\mathrm{AH}(X^p)^{1/p},$$

our series $G(-X^p)$ equals the reduction modulo p of $e_p(X)\,\mathrm{AH}(X^p)^{1/p}$. Consequently, for p odd, the product $G(X^p)\,G(-X^p)$ equals the reduction modulo p of

$$e_p(X)\,\mathrm{AH}(X^p)^{1/p}\cdot e_p(-X)\,\mathrm{AH}(-X^p)^{1/p},$$

which simplifies to $e_p(X)\,e_p(-X)$. Note that $e_p(X)\,\mathrm{AH}(X^p)^{1/p}$ belongs to $\mathbb{Z}_p[[X]]$ because $\mathrm{AH}(X)$ does. Hence so does $e_p(X)\,e_p(-X)$. □

Denote by $y^{\overline{n}} = y(y+1)\cdots(y+n-1)$ the *rising factorial*. The (unsigned) Stirling number of the first kind $\left[{n \atop i}\right]$, for $0 \le i \le n$, may be defined by the polynomial identity $y^{\overline{n}} = \sum_{i=0}^{n}\left[{n \atop i}\right] y^i$ in $\mathbb{Z}[y]$.

Proof of Proposition 4. In view of working modulo X^{p^2}, because $S(X)$ is congruent with $L_{p-1}^{(-X^p)}(X)$, we expand the latter as

$$L_{p-1}^{(-X^p)}(X) = \sum_{k=0}^{p-1}\binom{X^p-(k+1)}{p-1-k}\frac{X^k}{k!} = \sum_{k=0}^{p-1}(-1)^{k+1}(X^p+1)^{\overline{p-1-k}}X^k$$
$$= \sum_{k=0}^{p-1}\sum_{i=0}^{p-1-k}\left[{p-1-k \atop i}\right](X^p+1)^i(-1)^{k+1}X^k$$

$$= \sum_{k=0}^{p-1} \sum_{j=0}^{\infty} (-1)^{k+1} \left(\sum_{i=j}^{p-1-k} \begin{bmatrix} p-1-k \\ i \end{bmatrix} \binom{i}{j} \right) X^{pj+k}$$

$$= \sum_{k=0}^{p-1} \sum_{j=0}^{\infty} (-1)^{k+1} \begin{bmatrix} p-k \\ j+1 \end{bmatrix} X^{pj+k},$$

where we have used the standard identity $\sum_{t=m}^{n} \begin{bmatrix} n \\ t \end{bmatrix} \binom{t}{m} = \begin{bmatrix} n+1 \\ m+1 \end{bmatrix}$.

Because of Eq. (10) we have $L_{p-1}^{(-X^p)}(X)F(X^p) \equiv \mathrm{E}_p(X) \pmod{X^{p^2}}$, where $F(X^p) = \sum_{r=0}^{\infty} c_{rp} X^{rp}$ for some $c_{np} \in \mathbb{F}_p$. Comparing this with

$$L_{p-1}^{(-X^p)}(X)F(X^p) \equiv \sum_{k=0}^{p-1} \sum_{r=0}^{p-1} \sum_{j=0}^{r} (-1)^{k+1} \begin{bmatrix} p-k \\ j+1 \end{bmatrix} c_{(r-j)p} X^{rp+k} \pmod{X^{p^2}}$$

completes the proof. Note that the equation in the statement implicitly includes a definition of the coefficients c_{jp} when $k = 0$. □

Remark 8. The coefficients $u_n \in \mathbb{Q}$ of the Artin-Hasse series may be computed recursively from Eq. (6). When n is not a multiple of p, the recursive equation may be read modulo p, and hence applied directly to the coefficients a_n. Writing $n = rp + k$, with $0 \le k < p$, a recursive application of Eq. (6) shows that a_{rp+k} may eventually be computed from the coefficients a_{ip} for $i < r$. Proposition 4 provides an explicit form for the final result of that process.

Author contributions Both authors contributed jointly and equally to the paper.

Funding Open access funding provided by Università degli Studi di Milano - Bicocca within the CRUI-CARE Agreement.

Declarations

Conflict of interest The authors declare that they have no conflict of interest.

References

[1] Avitabile, M., Mattarei, S.: A generalized truncated logarithm. Aequationes Math. **93**(4), 711–734 (2019)
[2] Avitabile, M., Mattarei, S.: Grading switching for modular non-associative algebras. Lie algebras and related topics. Contemp. Math. Am. Math. Soc. **625**, 1–14 (2015)
[3] Avitabile, Marina, Mattarei, Sandro: Laguerre polynomials of derivations. Israel J. Math. **205**(1), 109–126 (2015)
[4] Avitabile, Marina, Mattarei, Sandro: Generalized finite polylogarithms. Glasgow Math. J. **63**(1), 66–80 (2021)
[5] Block, R.E., Wilson, R.L.: The simple Lie p-algebras of rank two. Ann. of Math. **115**(1), 93–168 (1982)
[6] Kanesaka, Kiyomi, Sekiguchi, Koji: Representation of Witt vectors by formal power series and its applications. Tokyo J. Math. **2**(2), 349–370 (1979)
[7] Mattarei, Sandro: Artin-Hasse exponentials of derivations. J. Algebra **294**(1), 1–18 (2005)
[8] Mattarei, Sandro: Exponential functions in prime characteristic. Aequationes Math. **71**(3), 311–317 (2006)
[9] Premet, A.A.: Cartan subalgebras of Lie p-algebras. Izv. Akad. Nauk SSSR Ser. Mat. **50**(4), 788-800-878–879 (1986)
[10] Winter, D.J.: On the toral structure of Lie p-algebras. Acta Math. **123**, 69–81 (1969)

Marina Avitabile
Dipartimento di Matematica e Applicazioni
Università degli Studi di Milano-Bicocca
via Cozzi 55
I-20125 Milano
Italy
e-mail: marina.avitabile@unimib.it

Sandro Mattarei
Charlotte Scott Centre for Algebra
University of Lincoln
Brayford Pool
Lincoln LN6 7TS
UK
e-mail: smattarei@lincoln.ac.uk

Received: August 30, 2023
Revised: August 30, 2023
Accepted: September 15, 2023