*Glasgow Math. J.* **63** (2021) 66–80. © The Author(s) 2020. Published by Cambridge University Press on behalf of Glasgow Mathematical Journal Trust.
doi:10.1017/S0017089520000026.

# GENERALIZED FINITE POLYLOGARITHMS

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, United Kingdom*
*e-mail: smattarei@lincoln.ac.uk*

(Received 7 May 2019; revised 11 October 2019; accepted 17 January 2020; first published online 19 February 2020)

**Abstract.** We introduce a generalization $\mathcal{L}_d^{(\alpha)}(X)$ of the finite polylogarithms $\mathcal{L}_d^{(0)}(X) = \mathcal{L}_d(X) = \sum_{k=1}^{p-1} X^k/k^d$, in characteristic $p$, which depends on a parameter $\alpha$. The special case $\mathcal{L}_1^{(\alpha)}(X)$ was previously investigated by the authors as the inverse, in an appropriate sense, of a parametrized generalization of the truncated exponential which is instrumental in a *grading switching* technique for nonassociative algebras. Here, we extend such generalization to $\mathcal{L}_d^{(\alpha)}(X)$ in a natural manner and study some properties satisfied by those polynomials. In particular, we find how the polynomials $\mathcal{L}_d^{(\alpha)}(X)$ are related to the powers of $\mathcal{L}_1^{(\alpha)}(X)$ and derive some consequences.

2010 *Mathematics Subject Classification*. Primary: 33E50; Secondary: 11G55, 39B52, 33C45

**1. Introduction.** In current terminology and notation introduced in [**4**], the *finite polylogarithms* are the polynomials $\mathcal{L}_d(X) = \sum_{k=1}^{p-1} X^k/k^d$, where $d$ is an integer, conveniently and most interestingly viewed in prime characteristic $p$. Although those polynomials, which are truncated versions of the series defining the classical polylogarithms, were already introduced by Mirimanoff [**10**] in his investigations on Fermat's Last Theorem, see [**11**, Lecture VIII], they have enjoyed renewed interest in recent years due to their connections with algebraic $K$-theory.

In this paper, we introduce a parametrized generalization of the finite polylogarithms. Our motivation stems from the occurrence of the special case $d = 1$ as an appropriate compositional inverse of generalized exponentials expressed by certain Laguerre polynomials. Those particular Laguerre polynomials were investigated by the authors in [**2**] as they play the role of generalized exponentials in a *grading switching* technique for modular, nonassociative algebras, whose purpose is to produce a new grading of an algebra from a given one. We limit ourselves here to giving the definition and exponential-like property of those Laguerre polynomials, referring the interested reader to a sketch of their role in grading switching in the Introduction of [**3**], and full details of that application in [**2**] and [**1**].

The Laguerre polynomials of interest here, regarded as having coefficients in the field $\mathbb{F}_p$ with $p$ elements, take the form

$$L_{p-1}^{(\alpha)}(X) = (1-\alpha^{p-1}) \sum_{k=0}^{p-1} \frac{X^k}{(1+\alpha)(2+\alpha)\cdots(k+\alpha)} \in \mathbb{F}_p[\alpha, X],$$

which specializes to the *truncated exponential* $E(X) = \sum_{k=0}^{p-1} X^k/k!$ when we set $\alpha = 0$. Note that despite the presence of denominators $L_{p-1}^{(\alpha)}(X)$ is indeed polynomial in $\alpha$ because $\alpha^{p-1} - 1 = \prod_{k=1}^{p-1}(\alpha + k)$ in $\mathbb{F}_p[\alpha]$. The crucial property of those Laguerre polynomials for the grading switching application is that they satisfy a congruence which is a weak version of the fundamental functional equation $\exp(X)\exp(Y) = \exp(X+Y)$ for the classical exponential series $\exp(X) = \sum_{k=0}^{\infty} X^k/k!$ in characteristic zero. Roughly speaking, the congruence relates the product $L_{p-1}^{(\alpha)}(X)L_{p-1}^{(\beta)}(Y)$ with $L_{p-1}^{(\alpha+\beta)}(X+Y)$, the latter multiplied by a polynomial in $\mathbb{F}_p(\alpha, \beta)[X, Y]$ whose most important feature in this context is that all its terms have total degree multiple of $p$. We quote that result from [**2**] in Theorem 1 and then supplement it with a more precise version, Theorem 2, where we provide explicit expressions for the coefficients of that polynomial. In order to provide a solid motivation for the particular generalization of finite polylogarithms that we intend to study here, which is inferred from the special case $d = 1$, we devote the remainder of Section 2 to proving that the exponential-like property described by Theorem 1 essentially characterizes the Laguerre polynomials under consideration. We formalize our conclusion in Theorem 3.

Thinking of $L_{p-1}^{(\alpha)}(X)$ as an exponential-like polynomial suggests that an appropriate compositional inverse $\pounds_1^{(\alpha)}(X)$ of $L_{p-1}^{(\alpha)}(X)$ may be interpreted as a logarithm-like polynomial. Such inverse was investigated in the paper [**3**], where it was denoted by $G^{(\alpha)}(X)$. However, to match the standard notation $\pounds_1(X)$ for the first finite polylogarithm, we set here $\pounds_1^{(\alpha)}(X) = -G^{(\alpha)}(X)$. The precise statement for $\pounds_1^{(\alpha)}(X)$ being (essentially) a left compositional inverse of $L_{p-1}^{(\alpha)}(X)$ then reads as $\pounds_1^{(\alpha)}(X)$ being the unique polynomial of degree less than $p$ in $\mathbb{F}_p(\alpha)[X]$ such that

$$-\pounds_1^{(\alpha)}\big(L_{p-1}^{(\alpha)}(X)\big) \equiv X \pmod{X^p - (\alpha^p - \alpha)}.$$

Before we give, in the next paragraph, an explicit description of the coefficients of $\pounds_1^{(\alpha)}(X)$, we wish to further stress that the above congruence is really what motivates its definition as a logarithm-like polynomial, as (essentially) the left inverse of the exponential-like polynomial $L_{p-1}^{(\alpha)}(X)$ (and also a right inverse with respect to an appropriate different modulus). In turn, the exponential-like property of $L_{p-1}^{(\alpha)}(X)$ determines that polynomial uniquely up to natural variations, as we mentioned above. Finally, the modulus of the above congruence is also natural and forced upon us by the application to grading switching. Altogether, this constitutes a strong support for this particular generalization of $\pounds_1(X) = \pounds_1^{(0)}(X)$ that we consider here. Setting $\alpha = 0$ the above congruence becomes $-\pounds_1\big(E(X)\big) \equiv X \pmod{X^p}$, which according to the functional equation $\pounds_1(1-X) = \pounds_1(X)$ (as polynomials in $\mathbb{F}_p[X]$) results from $\log\big(\exp(X)\big) = X$ upon viewing it first modulo $X^p$ and then modulo $p$. The details of this deduction are explained in the discussion following [**3**, Theorem 2].

It turns out that the coefficients of $\pounds_1^{(\alpha)}(X)$ can be explicitly described as follows. For integers $0 < k < p$ and $0 < a < p$, we let $p^{e(k,a)}$ be the highest power of $p$ which divides the product of binomial coefficients $\prod_{s=1}^{k} \binom{sa}{a}$, and set $g_k(\alpha) = \prod_{0<a<p}(1+\alpha/a)^{-e(k,a)}$, viewed as a rational function in $\mathbb{F}_p(\alpha)$. Then $\pounds_1^{(\alpha)}(X) = \sum_{k=1}^{p-1} g_k(\alpha)\, X^k/k$. This description of the coefficients $g_k(\alpha)$ of $\pounds_1^{(\alpha)}(X)$ is more compact than the original one we gave in [**3**,

https://doi.org/10.1017/S0017089520000026 Published online by Cambridge University Press

Subsection 2.2]. Most of the work to bring that description to the fully factorized and arguably more useful form given here was actually done in [**3**, Section 4], with a short supplementary argument which we provide in Subsection 3.2 of this paper.

To extend this generalization of $\pounds_1(X)$ to higher finite polylogarithms, we note that the various finite polylogarithms are connected one another by an application of the differential operator $X\,d/dX$. If this rule is to be preserved in the generalization, it is natural to set $\pounds_d^{(\alpha)}(X) = \sum_{k=1}^{p-1} g_k(\alpha)\, X^k/k^d$ for any integer $d$. Of course $\pounds_{d+p-1}^{(\alpha)}(X) = \pounds_d^{(\alpha)}(X)$. These polynomials in $\mathbb{F}_p(\alpha)[X]$, which generalize $\pounds_d(X) = \pounds_d^{(0)}(X)$, are the objects of interest in the remainder of the paper.

Functional equations for finite polylogarithms are of considerable interest, and we review some in Subsection 3.1. Some of them relate to a congruence which connects finite polylogarithms $\pounds_d(X)$ with powers of $\pounds_1(X)$, namely,

$$\pounds_1(X)^d \equiv (-1)^{d-1} d!\, \pounds_d(1-X) \pmod{X^p},$$

for $0 < d < p-1$, which is Equation 8 below. Our main result here is Theorem 5, which gives an extension of this congruence to our generalized finite polylogarithms $\pounds_d^{(\alpha)}(X)$. In the generalized version of the congruence (which in our formulation rather extends the above after $X$ is substituted with $1-X$), the right-hand side does not involve just $\pounds_d^{(\alpha)}(X)$ but is a linear combination of that and each lower one down to $\pounds_1^{(\alpha)}(X)$. Finally, we deduce a couple of consequences from Theorem 5, whose relevance we explain in Subsection 3.3. In particular, our final result, Theorem 7, gives an equation which expresses the finite polylogarithm $\pounds_d(X)$ as a linear combination of certain evaluations of all generalized finite polylogarithms $\pounds_d^{(r\alpha)}$ as $r$ varies from 1 to $p-1$. We collect all substantial proofs of our results on the generalized finite polylogarithms in the final Section 4.

**2. A generalized truncated exponential.** 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 $\alpha$ is a parameter, usually taken in the complex numbers. However, we may also view $L_n^{(\alpha)}(X)$ as a polynomial with rational coefficients in the two indeterminates $\alpha$ and $X$, hence in the polynomial ring $\mathbb{Q}[\alpha, X]$.

Having fixed a prime $p$, we are only interested in Laguerre polynomials of degree $n = p-1$, whose coefficients are $p$-integral and can be viewed modulo $p$. Throughout the paper, we work directly in characteristic $p$ rather than over the rationals, thus regarding $L_{p-1}^{(\alpha)}(X)$ as a polynomial in $\mathbb{F}_p[\alpha, X]$. The explicit form for $L_{p-1}^{(\alpha)}(X)$ mentioned in the introduction easily follows from the classical definition taking into account the identities $k!(p-1-k)! = (-1)^{k-1}$ for $0 \leq k < p$ and $\alpha^{p-1} - 1 = \prod_{k=1}^{p-1}(\alpha + k)$ in $\mathbb{F}_p[\alpha]$. We quote from [**2**] a congruence which we will use later

$$X\frac{d}{dX} L_{p-1}^{(\alpha)}(X) \equiv (X-\alpha) \cdot L_{p-1}^{(\alpha)}(X) \pmod{X^p - (\alpha^p - \alpha)}, \tag{1}$$

and that may be thought of as an analogue of the differential equation $\exp'(X) = \exp(X)$ for the classical exponential series. The differential equation for the polynomials $L_{p-1}^{(\alpha)}(X)$ stated in Equation 1 was used in [**2**] to prove the following analogue of the functional equation $\exp(X)\exp(Y) = \exp(X+Y)$.

https://doi.org/10.1017/S0017089520000026 Published online by Cambridge University Press

THEOREM 1 ([2, Proposition 2]). *Let $\alpha$, $\beta$, $X$, $Y$ be indeterminates over $\mathbb{F}_p$. There exist rational expressions $c_i(\alpha, \beta) \in \mathbb{F}_p(\alpha, \beta)$ such that*

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

*in $\mathbb{F}_p(\alpha, \beta)[X, Y]$, modulo the ideal generated by $X^p - (\alpha^p - \alpha)$ and $Y^p - (\beta^p - \beta)$.*

The actual statement of Proposition 2 in [2] is stronger and more involved than Theorem 1, as it had to provide a sharper control over the rational expressions $c_i(\alpha, \beta)$, which was required for an application to grading switching. The expressions $c_i(\alpha, \beta)$ are actually uniquely determined and are given by $c_0(\alpha, \beta) = -(\alpha - 1)_{p-1}(\beta - 1)_{p-1}/(\alpha + \beta - 1)_{p-1}$, and $c_i(\alpha, \beta) = -(\alpha - 1)_{p-1-i}(\beta - 1)_{i-1}/(\alpha + \beta - 1)_{p-1}$ for $0 < i < p$. Here, we are using the standard notation $(\gamma)_k = \gamma(\gamma - 1) \cdots (\gamma - k + 1)$ for the *falling factorials*, for $k$ a nonnegative integer, with the natural convention that $(\gamma)_0 = 1$. These explicit formulas were omitted from [2] as their available proof was awkward, but they will now follow from Theorem 2 below.

A simplification in those formulas and their proof results from a natural normalization of our Laguerre polynomials to turn their constant term into 1:

$$\mathcal{E}^{(\alpha)}(X) := \frac{L_{p-1}^{(\alpha)}(X)}{1 - \alpha^{p-1}} = \sum_{k=0}^{p-1} \frac{X^k}{(1+\alpha)(2+\alpha)\cdots(k+\alpha)} \in \mathbb{F}_p(\alpha)[X].$$

While $L_{p-1}^{(\alpha)}(X)$ has the advantage of having polynomial coefficients in $\alpha$, which was a mild simplification in its application to grading switching in [2], the polynomial $\mathcal{E}^{(\alpha)}(X)$ seems a more natural analogue of the exponential function. We now prove a more precise version of Theorem 1 in terms of $\mathcal{E}^{(\alpha)}(X)$, where the coefficients are given explicitly.

THEOREM 2. *Let $\alpha$, $\beta$, $X$, $Y$ be indeterminates over $\mathbb{F}_p$. Then*

$$\mathcal{E}^{(\alpha)}(X) \cdot \mathcal{E}^{(\beta)}(Y) \equiv \mathcal{E}^{(\alpha+\beta)}(X+Y) \cdot \left( 1 + \sum_{i=1}^{p-1} \frac{X^i Y^{p-i}}{(\alpha+i)_i \, (\beta+p-i)_{p-i}} \right)$$

*in $\mathbb{F}_p(\alpha, \beta)[X, Y]$, modulo the ideal generated by $X^p - (\alpha^p - \alpha)$ and $Y^p - (\beta^p - \beta)$.*

*Proof.* We know from Theorem 1 that there exist rational expressions $s_i(\alpha, \beta) \in \mathbb{F}_p(\alpha, \beta)$ such that

$$\mathcal{E}^{(\alpha)}(X) \cdot \mathcal{E}^{(\beta)}(Y) \equiv \mathcal{E}^{(\alpha+\beta)}(X+Y) \cdot \left( s_0(\alpha, \beta) + \sum_{i=1}^{p-1} s_i(\alpha, \beta) X^i Y^{p-i} \right)$$

in $\mathbb{F}_p(\alpha, \beta)[X, Y]$, modulo the ideal generated by $X^p - (\alpha^p - \alpha)$ and $Y^p - (\beta^p - \beta)$.

It will turn out that the expressions $s_i(\alpha, \beta)$ are actually uniquely determined and we will compute them by comparing coefficients of certain monomials in both sides of the above congruence, after reduction by the moduli. First, the only term in the product at the right-hand side of the congruence in which both exponents of $X$ and $Y$ are multiples of $p$ is $s_0(\alpha, \beta)$, hence comparing constant terms in both sides of the congruence we find $s_0(\alpha, \beta) = 1$.

Now compare the coefficients of $X^k$ in both sides of the congruence for $0 < k < p$. In the left-hand side, the coefficient equals $1/(\alpha + k)_k$. In the right-hand side, after reducing modulo $Y^p - (\beta^p - \beta)$, the coefficient of $X^k$ equals

https://doi.org/10.1017/S0017089520000026 Published online by Cambridge University Press

$$\frac{1}{(\alpha+\beta+k)_k} + \frac{\beta^p-\beta}{(\alpha+\beta+k)_k}\sum_{i=1}^{k}\binom{k}{i}s_i(\alpha,\beta).$$

Consequently, we find

$$(\beta^p-\beta)\sum_{i=1}^{k}\binom{k}{i}s_i(\alpha,\beta) = \frac{(\alpha+\beta+k)_k}{(\alpha+k)_k} - 1 = \frac{1}{(\alpha+k)_k}\sum_{i=1}^{k}\binom{k}{i}(\alpha+k)_{k-i}(\beta)_i,$$

where we have applied the *binomial theorem* for falling factorials, and hence

$$\sum_{i=1}^{k}\binom{k}{i}s_i(\alpha,\beta) = \sum_{i=1}^{k}\binom{k}{i}\frac{1}{(\alpha+i)_i(\beta+p-i)_{p-i}}.$$

This yields

$$s_i(\alpha,\beta) = \frac{1}{(\alpha+i)_i(\beta+p-i)_{p-i}}$$

for $0 < i < p$, as desired. □

The special case of Theorem 2 where $\alpha = \beta = 0$ concerns the truncated exponential $\mathcal{E}^{(0)}(X) = E(X)$ and is [**1**, Proposition 1], noting that $(i)_i\,(p-i)_{p-i} = i!(p-i)! \equiv (-1)^i i \pmod p$.

As we mentioned in Section 1, the existence of a congruence as in Theorem 1, for some unspecified rational expressions $c_i(\alpha,\beta)$, suffices to characterize the polynomials $L_{p-1}^{(\alpha)}(X)$ among the polynomials in $\mathbb{F}_p[\alpha][X]$, up to some natural variations. For convenience, we rather state and prove an essentially equivalent characterization of their scalar multiples $\mathcal{E}^{(\alpha)}(X)$, among the polynomials in $\mathbb{F}_p(\alpha)[X]$, again up to some natural variations.

THEOREM 3. *Let $\alpha, \beta, X, Y$ be indeterminates over $\mathbb{F}_p$ and let $P^{(\alpha)}(X)$ be a nonzero polynomial in $\mathbb{F}_p(\alpha)[X]$, of degree less than $p$. Suppose that there exist rational expressions $s_i(\alpha,\beta) \in \mathbb{F}_p(\alpha,\beta)$ such that*

$$P^{(\alpha)}(X)\cdot P^{(\beta)}(Y) \equiv P^{(\alpha+\beta)}(X+Y)\cdot\left(1+\sum_{i=1}^{p-1}s_i(\alpha,\beta)X^iY^{p-i}\right) \tag{2}$$

*in $\mathbb{F}_p(\alpha,\beta)[X,Y]$ modulo the ideal generated by $X^p-(\alpha^p-\alpha)$ and $Y^p-(\beta^p-\beta)$.*

*Assume that none of the denominators of the expressions $s_i(\alpha,\beta)$ has $\beta$ as a factor, so $s_i(\alpha,0)$ are defined. Assume also that $0$ is not a pole of $s_{p-1}(\alpha,0)$, nor of any coefficient of $P^{(\alpha)}(X)$, so $s_{p-1}(0,0)$ and $P^{(0)}(X)$ are defined.*

*Then $P^{(\alpha)}(X) = \mathcal{E}^{(c\alpha)}(cX)$ for some $c \in \mathbb{F}_p$.*

To avoid obscuring the argument of the proof, we have placed various assumptions in Theorem 3 on the denominators of the expressions $s_i(\alpha,\beta)$ and also of the coefficients of $P^{(\alpha)}(X)$. In another version of this result one may take $P^{(\alpha)}(X) \in \mathbb{F}_p[\alpha][X]$, hence with polynomial coefficients, rather than $P^{(\alpha)}(X) \in \mathbb{F}_p(\alpha)[X]$, provided that one allows a further rational expression $s_0(\alpha,\beta)$ in place of the term 1 in the right-hand side of the congruence. Then quite similar arguments as in the proof of Theorem 3 show that $P^{(\alpha)}(X) = d(\alpha)\cdot L_{p-1}^{(c\alpha)}(cX)$, for some polynomial $d(\alpha) \in \mathbb{F}_p[\alpha]$, and some $c \in \mathbb{F}_p$.

https://doi.org/10.1017/S0017089520000026 Published online by Cambridge University Press

*Proof.* The polynomial $P^{(\alpha)}(X)$ must have a nonzero constant term $P^{(\alpha)}(0)$. In fact, upon setting $Y = 0$ and $\beta = 0$, which is allowed according to our assumptions on the rational expressions $s_i(\alpha, \beta)$ and on $P^{(\alpha)}(X)$, Equation (2) yields $P^{(\alpha)}(X) \cdot P^{(0)}(0) \equiv P^{(\alpha)}(X)$ modulo $X^p - (\alpha^p - \alpha)$, whence $P^{(0)}(0) = 1$.

Because the only term in the product at the right-hand side of Equation (2) in which both exponents of $X$ and $Y$ are multiples of $p$ is the constant term $P^{(\alpha+\beta)}(0)$, we have $P^{(\alpha)}(0) \cdot P^{(\beta)}(0) = P^{(\alpha+\beta)}(0)$. Setting $\beta = k\alpha$ we find $P^{(\alpha)}(0) \cdot P^{(k\alpha)}(0) = P^{((k+1)\alpha)}(0)$, and working inductively we find $P^{(\alpha)}(0)^p = P^{(p\alpha)}(0) = P^{(0)}(0) = 1$, whence $P^{(\alpha)}(0) = 1$.

Following a standard approach to functional equations such as Equation (2), we apply the differential operator $d/dY$ to both sides. This is allowed for the congruence because $d/dY$ annihilates both $X^p - (\alpha^p - \alpha)$ and $Y^p - (\beta^p - \beta)$, and hence leaves invariant the ideal of $\mathbb{F}_p(\alpha, \beta)[X, Y]$ which they generate. Multiplying the resulting congruence by $X$ and specializing $Y = 0$ and $\beta = 0$, we find

$$X\,P^{(\alpha)}(X) \cdot c \equiv X\,\frac{dP^{(\alpha)}(X)}{dX} + s_{p-1}(\alpha, 0)P^{(\alpha)}(X)X^p \pmod{X^p - (\alpha^p - \alpha)},$$

where $c \in \mathbb{F}_p$ is the value of $dP^{(0)}(X)/dX$ at $X = 0$. After reducing by the modulus and rearranging terms this becomes

$$X\,\frac{dP^{(\alpha)}(X)}{dX} \equiv \big(cX - r(\alpha)\big)P^{(\alpha)}(X) \pmod{X^p - (\alpha^p - \alpha)},$$

where we have used the shorthand $r(\alpha) = (\alpha^p - \alpha)s_{p-1}(\alpha, 0)$. Note that $\alpha = 0$ is a zero of $r(\alpha)$, otherwise it would be a pole of $s_{p-1}(\alpha, 0) = r(\alpha)/(\alpha^p - \alpha)$, contrary to one of our assumptions. In particular, $r(\alpha)$ cannot be a nonzero constant.

If $c = 0$, then both sides of the congruence are polynomials of degree less than $p$, hence the congruence is actually an equality, and because $X\,dX^k/dX = kX^k$ it follows that $r(\alpha) = 0$ and $P^{(\alpha)}(X) = 1 = \mathcal{E}^{(0\alpha)}(0X)$.

Now assume that $c \neq 0$ and write $P^{(\alpha)}(X) = \sum_{k=0}^{p-1} c_k(\alpha)X^k$, hence with $c_0(\alpha) = 1$, and $c_1(0) = c$. After expanding the right-hand side and replacing the term $cX \cdot c_{p-1}(\alpha)X^{p-1}$ with $c \cdot c_{p-1}(\alpha) \cdot (\alpha^p - \alpha)$, the congruence becomes an equality as both sides have now degree less than $p$. Equating term by term, we find

$$\begin{cases} r(\alpha) = c \cdot c_{p-1}(\alpha) \cdot (\alpha^p - \alpha), & \text{and} \\ \big(r(\alpha) + k\big) \cdot c_k(\alpha) = c \cdot c_{k-1}(\alpha) & \text{for } 1 \le k \le p-1. \end{cases}$$

Because $r(\alpha)$ is not a nonzero constant, $r(\alpha) + k$ is never zero, and consequently none of the $c_k(\alpha)$ are zero.

As a preliminary step in solving this system for the rational expressions $c_k(\alpha)$, we note that the product of all $p$ equations reads

$$\big(r(\alpha)^p - r(\alpha)\big)\prod_{k=1}^{p-1} c_k(\alpha) = (\alpha^p - \alpha)c^p \prod_{k=1}^{p-1} c_k(\alpha).$$

Because $c^p = c$ this implies $\big(r(\alpha) - c\alpha\big)^p = r(\alpha) - c\alpha$, whence $r(\alpha) - c\alpha \in \mathbb{F}_p$. Because $r(0) = 0$ we deduce $r(\alpha) = c\alpha$. Solving

$$\begin{cases} \alpha = c_{p-1}(\alpha) \cdot (\alpha^p - \alpha), & \text{and} \\ \big(c\alpha + k\big) \cdot c_k(\alpha) = c \cdot c_{k-1}(\alpha) & \text{for } 1 \le k \le p-1, \end{cases}$$

https://doi.org/10.1017/S0017089520000026 Published online by Cambridge University Press

we conclude that $c_k(\alpha) = c^k/(c\alpha + k)_k$ for $0 \le k < p$, whence $P^{(\alpha)}(X) = \mathcal{E}^{(c\alpha)}(cX)$ as desired. □

We should mention that an earlier special version of the grading switching achieved in [2] through the Laguerre polynomials $L^{(\alpha)}_{p-1}(X)$ was devised in [6] using the *Artin-Hasse* exponential series $E_p(X) = \prod_{i=0}^{\infty} \exp(X^{p^i}/p^i)$. The coefficients of $E_p(X)$ are $p$-integral rational numbers and can therefore be viewed modulo $p$, so one may regard $E_p(X) \in \mathbb{F}_p[[X]]$ for the sake of its application to grading switching. The connection of the earlier theory based on the power series $E_p(X)$ with the more general one based on the polynomials $L^{(\alpha)}_{p-1}(X)$ is explained in [1, Proposition 6], but here we stress that the success of the former crucially depended on a property of $E_p(X)$ analogous to the property of $L^{(\alpha)}_{p-1}(X)$ described in Theorem 1: each term of the power series $E_p(X)E_p(Y)/E_p(X+Y) \in \mathbb{F}_p[[X, Y]]$ has total degree a multiple of $p$. It was then shown in [7] that this weak functional equation actually characterizes $E_p(X)$ in the power series ring $\mathbb{F}_p[[X]]$ up to certain natural variations. Theorem 3 matches that result for the Laguerre polynomials $L^{(\alpha)}_{p-1}(X)$, or their scalar multiples $\mathcal{E}^{(\alpha)}(X)$.

**3. Parametric versions of finite polylogarithms.** The finite polylogarithms $\mathrm{fl}_d(X) = \sum_{k=1}^{p-1} X^k/k^d$ are polynomial versions of the power series representations of the ordinary polylogarithms $\mathrm{Li}_d(X) = \sum_{k=1}^{\infty} X^k/k^d$, truncated as to make sense over a field of prime characteristic $p$. In this section, we extend the definition of finite polylogarithms to include a parameter $\alpha$, motivated by the case $d = 1$ which we extensively investigated in [3].

**3.1. Some properties of finite polylogarithms.** Before introducing our generalization $\mathrm{fl}^{(\alpha)}_d(X)$, we discuss some of the remarkable properties of the finite polylogarithms $\mathrm{fl}_d(X)$, including some which we aim to extend to our parametrized versions. Like their ordinary counterparts $\mathrm{Li}_d(X)$, finite polylogarithms satisfy a number of functional equations, which are more abundant for small positive values of $d$. In particular, $\mathrm{fl}_1(X)$, which is a truncated version of the power series for $-\log(1-X)$ satisfies $\mathrm{fl}_1(X) = -X^p \cdot \mathrm{fl}_1(1/X)$ and

$$\mathrm{fl}_1(X) = \mathrm{fl}_1(1-X). \tag{3}$$

Alternate application of these two equations yields six different equivalent representations for $\mathrm{fl}_1(X)$, see [3, Subsection 2.4] or [9, Section 6] for broader discussions. Those equations for $\mathrm{fl}_1(X)$ do not appear to directly relate to any properties of the logarithmic function (or series), but there is a two-variable functional equation which does, namely the *4-term relation*

$$\mathrm{fl}_1(X) - \mathrm{fl}_1(Y) + X^p \mathrm{fl}_1\left(\frac{Y}{X}\right) + (1-X)^p \mathrm{fl}_1\left(\frac{1-Y}{1-X}\right) = 0, \tag{4}$$

to be viewed as an identity in the polynomial ring $\mathbb{F}_p[X, Y]$. In fact, it is possible to view this equation as an analogue of the classical equation $\log(xy) = \log(x) + \log(y)$, in its equivalent form $-\log(1-X) - \log(1-Y) = \log((1-Y)/(1-X))$ in the power series ring $\mathbb{F}_p[[X, Y]]$, and actually derive it from that. See [3, Subsection 2.4] for a sketch of an argument and [9, Section 6] for two different full proofs of Equation (4) following this route.

A deeper connection between finite and ordinary polylogarithms was established by Elbaz-Vincent and Gangl in [4], stimulated by questions raised by Kontsevich [5], who

https://doi.org/10.1017/S0017089520000026 Published online by Cambridge University Press

had first exhibited a version of Equation (4) dubbing it the *generalized fundamental equation of information theory*. According to [**4**], many known functional equations for $\mathfrak{L}_d(X)$ are closely related to functional equations for the ordinary polylogarithms $\mathrm{Li}_{d+1}(X)$ (with index raised by one) and can be derived from the latter though a sort of *differential* or *infinitesimal* process. In particular, Equations (3) and (4) originate from functional equations for the dilogarithm $\mathrm{Li}_2(X)$, see [**4**, Proposition 5.9]. The same connection works for the functional equations which we are about to discuss, namely the only functional equations which exist for arbitrary $d$.

One functional equation valid for every $\mathfrak{L}_d(X)$ is the simple *inversion relation* [**4**, Proposition 5.7(1)],

$$\mathfrak{L}_d(X) = (-1)^d X^p \cdot \mathfrak{L}_d(1/X) \tag{5}$$

in $\mathbb{F}_p[X]$, whose special case $d = 1$ we have already mentioned. This is an immediate consequence of Wilson's theorem, $(p-1)! \equiv -1$ in $\mathbb{F}_p$ and says that the polynomials $\mathfrak{L}_d(X)$ are essentially self-reciprocal. The only other functional equation for $\mathfrak{L}_d(X)$ which exists for arbitrary $d$ is the *distribution relation* [**4**, Proposition 5.7(2)],

$$\mathfrak{L}_d(X^h) = h^{d-1} \sum_{j=0}^{|h|-1} \frac{1 - X^{ph}}{1 - \omega^{pj} X^p} \mathfrak{L}_d(\omega^j X), \tag{6}$$

where $\omega$ is a a primitive $h$th root of unity. This formulation of the distribution relation restricts the integer $h$ not to be a multiple of $p$, and Equation (6) formally takes place in $\mathbb{F}_q[X]$ for some finite field extension $\mathbb{F}_q$ containing such a root of unity, or in fact in its quotient field $\mathbb{F}_q(X)$ when $h$ is negative. (This restriction could be avoided by viewing the distribution relation as a congruence over a suitable number field rather than an equation over $\mathbb{F}_p$.) As pointed out in [**4**], Equation (5) may be viewed as the special case $h = -1$ of Equation (6).

When we view the distribution relation modulo $X^p - 1$, all summands vanish except for that with $j = 0$, and we find

$$\mathfrak{L}_d(X^h) \equiv h^d \mathfrak{L}_d(X) \pmod{X^p - 1} \tag{7}$$

in $\mathbb{F}_p[X]$, again for $h$ not a multiple of $p$. Replacing $X$ with $1 - X$, we can rewrite this in the equivalent form $\mathfrak{L}_d\big((1-X)^h\big) \equiv h^d \mathfrak{L}_d(1-X) \pmod{X^p}$. In the special case, where $d = 1$, this can be viewed as a congruence version of the property $\log(x^h) = h \log(x)$ of the logarithm.

Equation (7) can also be lifted from its special case $d = 1$ by means of a congruence relating finite polylogarithms $\mathfrak{L}_d(X)$ to powers of $\mathfrak{L}_1(X)$, namely,

$$\mathfrak{L}_1(X)^d \equiv (-1)^{d-1} d!\, \mathfrak{L}_d(1-X) \pmod{X^p}, \tag{8}$$

for $0 < d < p - 1$. This congruence, as well as much of the material on finite polylogarithms reviewed here, traces back to Mirimanoff [**10**], who developed it in his investigations on Fermat's Last Theorem, see [**11**, Lecture VIII, Equation (1,.27)]. A modern proof of a slightly sharper version modulo $X^{p+1}$ of Equation (8), which involves a Bernoulli number, can be found in [**8**, Lemma 3.2]. When $d = 1$ Equation (8) is a consequence of Equation (3), and when $d = 2$ or 3 it can be strengthened to exact functional equations (meaning equalities, not just congruences) by adding suitable extra terms, see [**8**, Equations (14) and (15)], also already known to Mirimanoff. A way of deriving those functional equations for $d = 2, 3$ from Equation (8) by the sole use of symmetries is given

https://doi.org/10.1017/S0017089520000026 Published online by Cambridge University Press

in [8, Section 3]. However, no such refinement is known (or likely even exists) for larger values of $d$.

**3.2. Generalized finite polylogarithms.** We recall our generalization $\mathfrak{L}_d^{(\alpha)}(X)$ of finite polylogarithms which we anticipated in Section 1. For integers $0 < k < p$ and $0 < a < p$, we let $p^{e(k,a)}$ be the highest power of $p$ which divides the product of binomial coefficients $\prod_{s=1}^{k} \binom{sa}{a}$ and set $g_k(\alpha) = \prod_{0<a<p} (1+\alpha/a)^{-e(k,a)}$, viewed as a rational function in $\mathbb{F}_p(\alpha)$. Then for any integer $d$, we set

$$\mathfrak{L}_d^{(\alpha)}(X) = \sum_{k=1}^{p-1} g_k(\alpha)\, X^k/k^d.$$

This definition has its roots in the special case $d = 1$, where $\mathfrak{L}_1^{(\alpha)}(X)$ is a left compositional inverse of $L_{p-1}^{(\alpha)}(X)$ in the context of the previous section, namely it satisfies

$$-\mathfrak{L}_1^{(\alpha)}\big(L_{p-1}^{(\alpha)}(X)\big) \equiv X \pmod{X^p - (\alpha^p - \alpha)}.$$

Thus, $\mathfrak{L}_1^{(\alpha)}(X)$ serves a generalization of the truncated logarithm $\mathfrak{L}_1(X) = \mathfrak{L}_1^{(0)}(X)$ matching the way $L_{p-1}^{(\alpha)}(X)$ generalizes the truncated exponential. This definition of $\mathfrak{L}_1^{(\alpha)}(X)$ extends naturally to $\mathfrak{L}_d^{(\alpha)}(X)$ by imposing that they have no constant term and they satisfy $(X\, d/dX)\mathfrak{L}_d^{(\alpha)}(X) = \mathfrak{L}_{d-1}^{(\alpha)}(X)$ for all integers $d$, which is the way ordinary truncated polylogarithms $\mathfrak{L}_d(X)$ are related. Because $\mathfrak{L}_{d+p-1}^{(\alpha)}(X) = \mathfrak{L}_d^{(\alpha)}(X)$, we can assume $0 \le d < p-1$ in the sequel. Also, the case of $p = 2$ is uninteresting as then $\mathfrak{L}_d^{(\alpha)}(X) = X$ for all $d$, and so we assume $p$ odd throughout this section.

The coefficients $g_k(\alpha)$ originally arose in [3] as $g_k(\alpha) = 1/\prod_{s=1}^{k-1} b_{1,s}(\alpha)$, with the polynomials $b_{1,s}(\alpha) \in \mathbb{F}_p[\alpha]$ defined as

$$b_{1,s}(\alpha) = \sum_{k=0}^{p-1} (-1/s)^k \binom{\alpha - 1}{p-1-k} \binom{s\alpha - 1}{k},$$

for $0 < s < p-1$. As explained there they can be viewed as special values of certain Jacobi polynomials, but what matters here are their full factorizations in $\mathbb{F}_p[\alpha]$, which were found in [3]. According to [3, Lemma 11], those polynomials satisfy

$$b_{1,s}(\alpha) b_{1,s}(-\alpha) = 1 - \alpha^{p-1}, \tag{9}$$

whence each has degree $(p-1)/2$, which was not obvious from their definition as sums. Furthermore, the equation implies that $b_{1,s}(\alpha)$ factorizes into products of distinct linear factors in $\mathbb{F}_p[\alpha]$, and exactly one of each pair of opposite nonzero elements of $\mathbb{F}_p$ is a root. A simple characterization of which elements of $\mathbb{F}_p$ are roots of $b_{1,s}(\alpha)$ was given in [3, Theorem 12], and for completeness we now show how that leads to the definition of the rational functions $g_k(\alpha)$ which we gave above.

LEMMA 4. *For $0 < k < p$, we have $g_k(\alpha) = 1/\prod_{s=1}^{k-1} b_{1,s}(\alpha)$.*

*Proof.* Each polynomial $b_{1,s}(\alpha)$ has constant term $b_{1,s}(0) = \sum_{k=0}^{p-1} (-1)^k (1/s)^k = 1$, hence its factorization in $\mathbb{F}_p[\alpha]$ is completely described by its roots. According to [3, Theorem 12], in its alternate formulation given in [3, Remark 13], an integer $0 < a < p$ is a root of $b_{1,s}(\alpha)$ (when interpreted as its image in $\mathbb{F}_p$) precisely when $p$ does not divide the

https://doi.org/10.1017/S0017089520000026 Published online by Cambridge University Press

binomial coefficient $\binom{a+sa}{a}$. Equivalently, $-a$ is a root of $b_{1,s}(\alpha)$ precisely when $p$ divides the binomial coefficient $\binom{a+sa}{a}$. Now note that $p^2$ cannot divide $\binom{a+sa}{a}$ and the conclusion follows. □

**3.3. Congruential functional equations for $\mathfrak{L}_d^{(\alpha)}(X)$.** The main goal of the remainder of this paper is to provide analogues for our generalized finite polylogarithms $\mathfrak{L}_d^{(\alpha)}(X)$ of some of the known relations among finite polylogarithms defined for generic $d$, which we summarized in Subsection 3.1. Thus, besides the easy Equation (5) we will generalize Equation (8), and then use that to generalize Equation (7). We will state our results here and prove them in the next section.

We assign a name to a polynomial which will occur repeatedly, namely,

$$T(X) := L_{p-1}^{(X^p)}(X^p - X) = \prod_{i=1}^{p-1}(1 + X/i)^i, \tag{10}$$

where the explicit factorization given was proved in [**2**, Lemma 1]. This polynomial will occur in the modulus $X^p - T(\alpha)$ of various congruences involving $\mathfrak{L}_d^{(\alpha)}(X)$, but also, for example, in an expression for the highest coefficient of $\mathfrak{L}_d^{(\alpha)}(X)$, because $g_{p-1}(\alpha) = (1 - \alpha^{p-1})/T(\alpha)$. This was proved in [**3**, Corollary 16], but can also be easily shown directly from our definition of $g_{p-1}(\alpha)$, as we explain now as an example of such evaluations.

According to Lucas' theorem on binomial coefficients modulo a prime, $p$ divides the factor $\binom{sa}{a}$ in our definition of $g_k(\alpha)$ precisely when the (least nonnegative) remainder of dividing $(s-1)a$ by $p$ is not less than $p - a$. In the case of $g_{p-1}(\alpha)$ the remainders of dividing $(s-1)a$ by $p$, for a given $a$ as $s$ ranges over $0 < s < p$, will take all values from 0 to $p - 1$ with the exception of $p - a$, hence precisely $a - 1$ of them will exceed $p - a$. Therefore, we find $g_{p-1}(\alpha) = \prod_{a=1}^{p-1}(1 - \alpha/a)^{-a+1}$ as desired.

Another relation among the coefficients $g_k(\alpha)$ amounts to the symmetry relation $b_{1,s}(\alpha) = b_{1,p-1-s}(\alpha)$ of [**3**, Corollary 14], for $0 < s < p - 1$. Taken together, in terms of the polynomials $g_k(\alpha)$, those equations are equivalent to

$$g_k(\alpha) \cdot g_{p-k}(\alpha) = g_{p-1}(\alpha), \qquad \text{for } 0 < k < p. \tag{11}$$

As a consequence of this symmetry together with Equation (9), one has

$$T(\alpha) \cdot \mathfrak{L}_d^{(\alpha)}(X) = (-1)^d X^p \cdot \mathfrak{L}_d^{(-\alpha)}\left(\frac{1 - \alpha^{p-1}}{X}\right),$$

a generalization of Equation (5) which can be proved in the same way as its special case $d = 1$ in [**3**, Theorem 6].

Our main result on generalized polylogarithms is a generalization of Equation (8). This generalized version does not relate $\mathfrak{L}_1^{(\alpha)}(X)^d$ to $\mathfrak{L}_d^{(\alpha)}(X)$ alone, but also involves lower polylogarithms. Denoting by $\left[{n \atop k}\right]$ the (unsigned) Stirling number of the first kind, which for $0 < k \le n$ may be characterized by the polynomial identities $(X + n - 1)_n = \sum_{k=1}^{n} \left[{n \atop k}\right] X^k$ in $\mathbb{Z}[X]$, we have the following result.

THEOREM 5. *For any $0 < d < p - 1$, we have*

$$\frac{\mathfrak{L}_1^{(\alpha)}(X)^d}{d} \equiv (-1)^{d-1} \sum_{r=0}^{d-1} \left[{d \atop r+1}\right] \alpha^r \mathfrak{L}_{d-r}^{(\alpha)}(X) \pmod{X^p - T(\alpha)}$$

*in the polynomial ring $\mathbb{F}_p(\alpha)[X]$.*

https://doi.org/10.1017/S0017089520000026 Published online by Cambridge University Press

In its specialization at $\alpha = 0$, because $\left[\begin{smallmatrix} d \\ 1 \end{smallmatrix}\right] = (d-1)!$ Theorem 5 reads $\mathfrak{L}_1(X)^d \equiv (-1)^{d-1} d!\, \mathfrak{L}_d(X) \pmod{X^p - 1}$. We recover Equation (8) by replacing $X$ with $1 - X$ and taking equation $\mathfrak{L}_1(X) = \mathfrak{L}_1(1 - X)$ into account.

The congruence of Theorem 5 can be extended to $d = p - 1$ but requires an extra term $1 - \alpha^{p-1}$ at the right-hand side in that case. Because $\left[\begin{smallmatrix} p-1 \\ k \end{smallmatrix}\right] \equiv 1 \pmod{p}$ for $0 < k < p$, the congruence for $d = p - 1$ reads

$$\mathfrak{L}_1^{(\alpha)}(X)^{p-1} \equiv 1 - \alpha^{p-1} + \sum_{r=0}^{p-2} \alpha^r \mathfrak{L}_{p-1-r}^{(\alpha)}(X) \pmod{X^p - T(\alpha)}.$$

Our next result generalizes Equation (7). Its special case where $d = 1$ is [3, Theorem 8], and we use Theorem 5 to extend that to higher values of $d$.

THEOREM 6. *For $0 < h < p$ and $0 < d < p - 1$, we have*

$$\mathfrak{L}_d^{(h\alpha)}\big(g_h(\alpha) X^h\big) \equiv h^d \mathfrak{L}_d^{(\alpha)}(X) \pmod{X^p - T(\alpha)}$$

*in the polynomial ring $\mathbb{F}_p(\alpha)[X]$.*

Our final result combines evaluations of all generalized finite polylogarithms $\mathfrak{L}_d^{(r\alpha)}$ as $r$ varies from 1 to $p - 1$ and relates them to the standard finite polylogarithm $\mathfrak{L}_d(X)$. To avoid having to extend the ground field with $\alpha^{1/p}$, we conveniently replace $\alpha$ with $\alpha^p$ in the statement.

THEOREM 7. *For any integer $d$, we have*

$$\sum_{r=1}^{p-1} \mathfrak{L}_d^{(r\alpha^p)}\big(T(r\alpha)\, X\big) = (\alpha^{p-1} - 1)\mathfrak{L}_d(X)$$

*in the polynomial ring $\mathbb{F}_p(\alpha)[X]$.*

Note that Theorem 7 states an identity, not just a congruence. Because $\mathfrak{L}_d^{(0)}(X) = \mathfrak{L}_d(X)$ and $T(0) = 1$ that can also be written as

$$\sum_{r=0}^{p-1} \mathfrak{L}_d^{(r\alpha^p)}\big(T(r\alpha)\, X\big) = \alpha^{p-1} \mathfrak{L}_d(X).$$

In a sense, the special case $d = 1$ of Theorem 7 gives a rather trivial answer to Question 7 in [3], which asked for a generalization of the functional equation $\mathfrak{L}_1(1 - X) = \mathfrak{L}_1(X)$ for the polynomials $\mathfrak{L}_1^{(\alpha)}(X)$, possibly involving various values of $\alpha$: when $d = 1$ the left-hand side of the equation of Theorem 7 is invariant under the substitution $X \mapsto 1 - X$, because the right-hand side is. A subtler answer appears now unlikely.

**4. Proofs of Theorem 5, Theorem 6, and Theorem 7 .** Our proof of Theorem 5 will proceed by applying the differential operator $X\, d/dX$ to the desired congruence, whence the left-hand side will give $\mathfrak{L}_0^{(\alpha)}(X) \cdot \mathfrak{L}_1^{(\alpha)}(X)^{d-1}$. Working inductively, a crucial step will be expressing the product of $\mathfrak{L}_0^{(\alpha)}(X)$ and $\mathfrak{L}_1^{(\alpha)}(X)$ as a linear combination of them, which is what the next congruence achieves.

LEMMA 8. *The product $\mathfrak{L}_0^{(\alpha)}(X) \cdot \mathfrak{L}_1^{(\alpha)}(X)$ satisfies the congruence*

$$\mathfrak{L}_0^{(\alpha)}(X) \cdot \mathfrak{L}_1^{(\alpha)}(X) \equiv -\mathfrak{L}_1^{(\alpha)}(X) - \alpha \mathfrak{L}_0^{(\alpha)}(X) \pmod{X^p - T(\alpha)}$$

*in the polynomial ring $\mathbb{F}_p(\alpha)[X]$.*

https://doi.org/10.1017/S0017089520000026 Published online by Cambridge University Press

*Proof.* We apply the differential operator $d/dX$ to both sides of the congruence

$$-\pounds_1^{(\alpha)}(L_{p-1}^{(\alpha)}(X)) \equiv X \pmod{X^p - (\alpha^p - \alpha)}, \tag{12}$$

using Equations (1) and $(X\,d/dX)\pounds_d^{(\alpha)}(X) = \pounds_{d-1}^{(\alpha)}(X)$. Noting that both $X$ and $L_{p-1}^{(\alpha)}(X)$ are coprime with the modulus, the latter because of Equation (10), and hence are invertible in the quotient ring $\mathbb{F}_p(\alpha)[X]/\big(X^p - (\alpha^p - \alpha)\big)$, we find

$$-\frac{1}{L_{p-1}^{(\alpha)}(X)}\pounds_0^{(\alpha)}\big(L_{p-1}^{(\alpha)}(X)\big) \cdot \frac{X-\alpha}{X} L_{p-1}^{(\alpha)}(X) \equiv 1 \pmod{X^p - (\alpha^p - \alpha)}.$$

After cancellation and multiplication by $X$, we obtain

$$-\pounds_0^{(\alpha)}\big(L_{p-1}^{(\alpha)}(X)\big) \cdot (X - \alpha) \equiv X \pmod{X^p - (\alpha^p - \alpha)}.$$

Now we would like to regard $L_{p-1}^{(\alpha)}(X)$ as a new variable, but this will require a foray into a power series ring in a similar fashion as in the proofs of Corollary 3 and Theorem 8 in [**3**]. Thus, we extend the ground field to $\mathbb{F}_p(\alpha^{1/p})$, where $X^p - (\alpha^p - \alpha)$ becomes a $p$th power, and after setting $X = x + \alpha - \alpha^{1/p}$ the congruence we have found reads

$$-\pounds_0^{(\alpha)}\big(L_{p-1}^{(\alpha)}(x + \alpha - \alpha^{1/p})\big) \cdot (x - \alpha^{1/p}) \equiv x + \alpha - \alpha^{1/p} \pmod{x^p}, \tag{13}$$

in the polynomial ring $\mathbb{F}_p(\alpha^{1/p})[x]$. In the same way, Equation (12) is equivalent to the congruence

$$-\pounds_1^{(\alpha)}\big(L_{p-1}^{(\alpha)}(x + \alpha - \alpha^{1/p})\big) - (\alpha - \alpha^{1/p}) \equiv x \pmod{x^p} \tag{14}$$

in the polynomial ring $\mathbb{F}_p(\alpha^{1/p})[x]$. However, both congruences can and will now be interpreted in the power series ring $\mathbb{F}_p(\alpha^{1/p})[[x]]$.

Set $\delta = T(\alpha^{1/p})$ and

$$X = -L_{p-1}^{(\alpha)}(x + \alpha - \alpha^{1/p}) + \delta, \tag{15}$$

where we are reusing the symbol $X$ with a different meaning from earlier in the proof. Because the polynomial $X \in \mathbb{F}_p(\alpha^{1/p})[x]$ has no constant term and a nonzero term of degree one, when viewed as a power series in $\mathbb{F}_p(\alpha^{1/p})[[x]]$ it generates its maximal ideal $(x)$. In particular, $X$ has a compositional inverse as a series in $\mathbb{F}_p(\alpha^{1/p})[[x]]$, meaning that Equation (15) can be inverted to express $x$ as a power series in $X$ and we may view $\mathbb{F}_p(\alpha^{1/p})[[x]]$ as the power series ring $\mathbb{F}_p(\alpha^{1/p})[[X]]$. According to Equation (14), such inverse satisfies

$$x \equiv -\pounds_1^{(\alpha)}(\delta - X) - (\alpha - \alpha^{1/p}) \pmod{X^p},$$

where we have taken advantage of $(X^p) = (x^p)$. Substituting this into Equation (13), we find

$$-\pounds_0^{(\alpha)}(\delta - X) \cdot \big(-\pounds_1^{(\alpha)}(\delta - X) - \alpha\big) \equiv -\pounds_1^{(\alpha)}(\delta - X) \pmod{X^p}.$$

Because this congruence involves only polynomials, it actually takes place in the polynomial ring $\mathbb{F}_p(\alpha^{1/p})[X]$. Replacing $X$ with $\delta - X$, we have

$$\pounds_0^{(\alpha)}(X)\big(\pounds_1^{(\alpha)}(X) + \alpha\big) \equiv -\pounds_1^{(\alpha)}(X) \pmod{X^p - T(\alpha)},$$

which is equivalent to the desired conclusion. □

https://doi.org/10.1017/S0017089520000026 Published online by Cambridge University Press

We are now ready to present a proof of Theorem 5.

*Proof of Theorem 5.* We will omit the modulus from all congruences in this proof, which will invariably be $X^p - T(\alpha)$. We proceed by induction on $d$, the case $d = 1$ being trivial, hence assume $d > 1$. Because

$$\sum_{r=0}^{d-1} \begin{bmatrix} d \\ r+1 \end{bmatrix} (k\alpha)^r = (k\alpha + d - 1)_d/(k\alpha) = (k\alpha + d - 1)_{d-1},$$

the desired conclusion can be written as

$$\pounds_1^{(\alpha)}(X)^d/d \equiv (-1)^{d-1} \sum_{k=1}^{p-1} (k\alpha + d - 1)_{d-1}\, g_k(\alpha) X^k/k^d.$$

To prove this congruence, write

$$\pounds_1^{(\alpha)}(X)^d/d \equiv \sum_{k=0}^{p-1} c_k(\alpha) X^k,$$

as certainly holds for certain rational expressions $c_k(\alpha) \in \mathbb{F}_p(\alpha)$ to be determined. Applying the differential operator $X\, d/dX$ to both sides of the congruence, we find

$$\pounds_0^{(\alpha)}(X) \cdot \pounds_1^{(\alpha)}(X)^{d-1} \equiv \sum_{k=1}^{p-1} k c_k(\alpha) X^k.$$

Note that this kills the coefficient $c_0(\alpha)$, so we will deal with that separately later. According to Lemma 8, the above congruence is equivalent to

$$-\pounds_1^{(\alpha)}(X)^{d-1} - \alpha \pounds_0^{(\alpha)}(X) \pounds_1^{(\alpha)}(X)^{d-2} \equiv \sum_{k=1}^{p-1} k c_k(\alpha) X^k.$$

Now by the inductive hypothesis, we have

$$\pounds_1^{(\alpha)}(X)^{d-1} \equiv (-1)^d (d-1) \sum_{k=1}^{p-1} (k\alpha + d - 2)_{d-2}\, g_k(\alpha) X^k/k^{d-1},$$

and because $\pounds_0^{(\alpha)}(X) \pounds_1^{(\alpha)}(X)^{d-2}$ results from applying the differential operator $X\, d/dX$ to $\pounds_1^{(\alpha)}(X)^{d-1}/(d-1)$, we obtain

$$\pounds_0^{(\alpha)}(X) \pounds_1^{(\alpha)}(X)^{d-2} \equiv (-1)^d \sum_{k=1}^{p-1} (k\alpha + d - 2)_{d-2}\, g_k(\alpha) X^k/k^{d-2}.$$

In conclusion, we find

$$\begin{aligned} k\, c_k(\alpha) &= (-1)^{d-1} (k\alpha + d - 2)_{d-2} (d - 1 + k\alpha)\, g_k(\alpha)/k^{d-1} \\ &= (-1)^{d-1} (k\alpha + d - 1)_{d-1}\, g_k(\alpha)/k^{d-1}, \end{aligned}$$

for $1 \le k \le p - 1$.

https://doi.org/10.1017/S0017089520000026 Published online by Cambridge University Press

In order to complete the proof, it remains to show that $c_0(\alpha)$ vanishes. Using the inductive hypothesis, it suffices to show that

$$\pounds_1^{(\alpha)}(X) \cdot \sum_{k=1}^{p-1} (k\alpha + d - 2)_{d-2}\, g_k(\alpha) X^k / k^{d-1}$$

has no term of degree $p$, as that is the only term which would contribute to $c_0(\alpha)$ after reduction modulo $X^p - T(\alpha)$. In fact, the coefficient of $X^p$ in the above product equals

$$\sum_{k=1}^{p-1} \frac{g_{p-k}(\alpha)}{p-k} \cdot \frac{g_k(\alpha)(k\alpha + d - 2)_{d-2}}{k^{d-1}} = g_{p-1}(\alpha) \sum_{k=1}^{p-1} \frac{(k\alpha + d - 2)_{d-2}}{k^d},$$

where we have used Equation (11). The latter sum vanishes because $\sum_{k=1}^{p-1} 1/k^r$ vanishes in $\mathbb{F}_p$ for $0 < r < p-1$ and $(k\alpha + d - 2)_{d-2}$ has degree less than $p-1$ as polynomial in $k$. □

When $d = p-1$, a supplementary case which we mentioned after Theorem 5, the inductive step extends in the above proof providing expressions for the coefficients $c_k(\alpha)$ for $0 < k < p$, but the separate final argument for the vanishing of $c_0(\alpha)$ needs modifications, and yields $c_0(\alpha) = \alpha^{p-1} - 1$ instead.

The following proof of Theorem 6 relies on the special case where $d = 1$, which is [**3**, Theorem 8], and uses Theorem 5 to extend it to higher values of $d$.

*Proof of Theorem 6.* We proceed by induction on $d$, the case $d = 1$ being [**3**, Theorem 8]. Hence, assume $1 < d < p-1$ and consider the right-hand side of the desired congruence multiplied by $d!$ to avoid introducing denominators. According to Theorem 5,

$$d!\, h^d \pounds_d^{(\alpha)}(X) \equiv (-1)^{d-1} (h\pounds_1^{(\alpha)}(X))^d - d \sum_{r=1}^{d-1} \begin{bmatrix} d \\ r+1 \end{bmatrix} (h\alpha)^r h^{d-r} \pounds_{d-r}^{(\alpha)}(X)$$

modulo $X^p - T(\alpha)$. By induction, we have

$$h^{d-r} \pounds_{d-r}^{(\alpha)}(X) \equiv \pounds_{d-r}^{(h\alpha)}\left(g_h(\alpha) X^h\right) \pmod{X^p - T(\alpha)}$$

for $0 < r < d$, and hence $d!\, h^d \pounds_d^{(\alpha)}(X)$ is congruent to

$$(-1)^{d-1} \left(\pounds_1^{(h\alpha)}\left(g_h(\alpha) X^h\right)\right)^d - d \sum_{r=1}^{d-1} \begin{bmatrix} d \\ r+1 \end{bmatrix} (h\alpha)^r \pounds_{d-r}^{(h\alpha)}\left(g_h(\alpha) X^h\right)$$

modulo $X^p - T(\alpha)$. According to Theorem 5, with $X$ replaced by $g_h(\alpha) X^h$ and $\alpha$ replaced by $h\alpha$, the above expression is congruent to the desired $d!\, \pounds_d^{(h\alpha)}\left(g_h(\alpha) X^h\right)$, but modulo $\left(g_h(\alpha) X^h\right)^p - T(h\alpha)$. However, this polynomial is a multiple of the desired modulus $X^p - T(\alpha)$ because $T(h\alpha) = g_h(\alpha)^p\, T(\alpha)^h$. This can be seen by setting $X = \alpha - \alpha^{1/p}$ in the congruence

$$g_h(\alpha) \left(L_{p-1}^{(\alpha)}(X)\right)^h \equiv L_{p-1}^{(h\alpha)}(hX) \pmod{X^p - (\alpha^p - \alpha)},$$

which is [**3**, Equation 6], and then taking $p$th powers of both sides. □

We conclude the paper with a proof of Theorem 7, which also uses Lemma 8.

https://doi.org/10.1017/S0017089520000026 Published online by Cambridge University Press

*Proof of Theorem 7.* Expanding the left-hand side of the claimed equation, we find

$$\sum_{r=1}^{p-1} \mathcal{L}_d^{(r\alpha^p)}\big(T(r\alpha)\,X\big) = \sum_{k=1}^{p-1}\Bigg(\sum_{r=1}^{p-1} g_k(r\alpha^p)\,T(r\alpha)^k\Bigg)X^k/k^d.$$

As mentioned in the proof of Theorem 6, we have $T(h\alpha) = g_h(\alpha^p)\,T(\alpha)^h$ for $0 < h < p$, whence $g_k(r\alpha^p)\,T(r\alpha)^k = T(kr\alpha) = g_r(k\alpha^p)\,T(k\alpha)^r$. Consequently, we have

$$\sum_{r=1}^{p-1} g_k(r\alpha^p)\,T(r\alpha)^k = \sum_{r=1}^{p-1} g_r(k\alpha^p)\,T(k\alpha)^r = \mathcal{L}_0^{(k\alpha^p)}\big(T(k\alpha)\big).$$

Computing this reduces to computing $\mathcal{L}_1^{(\alpha^p)}\big(T(\alpha)\big)$ by means of Lemma 8. In fact, after taking $p$th powers of both sides the congruence of Lemma 8 yields

$$\mathcal{L}_0^{(\alpha^p)}(X^p)\cdot\mathcal{L}_1^{(\alpha^p)}(X^p) \equiv -\mathcal{L}_1^{(\alpha^p)}(X^p) - \alpha^p\mathcal{L}_0^{(\alpha^p)}(X^p) \pmod{X^p - T(\alpha)},$$

whence

$$\mathcal{L}_0^{(\alpha^p)}\big(T(\alpha)\big)\cdot\mathcal{L}_1^{(\alpha^p)}\big(T(\alpha)\big) = -\mathcal{L}_1^{(\alpha^p)}\big(T(\alpha)\big) - \alpha^p\mathcal{L}_0^{(\alpha^p)}\big(T(\alpha)\big)$$

in $\mathbb{F}_p[\alpha]$. Now taking $p$th powers of both sides of the congruence $-\mathcal{L}_1^{(\alpha)}\big(L_{p-1}^{(\alpha)}(X)\big) \equiv X \pmod{X^p - (\alpha^p - \alpha)}$ and then replacing $X^p$ with $\alpha^p - \alpha$, we find $\mathcal{L}_1^{(\alpha^p)}\big(T(\alpha)\big) = \alpha - \alpha^p$. Consequently, we find $\mathcal{L}_0^{(\alpha^p)}\big(T(\alpha)\big) = \alpha^{p-1} - 1$, whence $\mathcal{L}_0^{(k\alpha^p)}\big(T(k\alpha)\big) = \alpha^{p-1} - 1$, as desired. □

## REFERENCES


**1.** M. Avitabile and S. Mattarei, *Grading switching for modular non-associative algebras*, Lie algebras and related topics, Contemp. Math., vol. 652, Amer. Math. Soc., Providence, RI, 2015, pp. 1–14. MR 3453046

**2.** M. Avitabile and S. Mattarei, *Laguerre polynomials of derivations*, Israel J. Math. **205** (2015), no. 1, 109–126. MR 3314584

**3.** M. Avitabile and S. Mattarei, *A generalized truncated logarithm*, Aequationes Math. **93** (2019), no. 4, 711–734. MR 3984323

**4.** P. Elbaz-Vincent and H. Gangl, *On poly(ana)logs. I*, Compositio Math. **130** (2002), no. 2, 161–210. MR 1883818 (2002m:11059)

**5.** M. Kontsevich, *The $1\frac{1}{2}$-logarithm. Appendix to: "On poly(ana)logs. I" [Compositio Math* **130** *(2002), no. 2, 161–210; MR1883818 (2002m:11059)] by P. Elbaz-Vincent and H. Gangl*, Compositio Math. **130** (2002), no. 2, 211–214. MR 1884238 (2002m:11060)

**6.** S. Mattarei, *Artin-Hasse exponentials of derivations*, J. Algebra **294** (2005), no. 1, 1–18. MR 2171626

**7.** S. Mattarei, *Exponential functions in prime characteristic*, Aequationes Math. **71** (2006), no. 3, 311–317. MR 2236408 (2007b:39056)

**8.** S. Mattarei and R. Tauraso, *Congruences for central binomial sums and finite polylogarithms*, J. Number Theory **133** (2013), no. 1, 131–157. MR 2981405

**9.** S. Mattarei and R. Tauraso, *From generating series to polynomial congruences*, J. Number Theory **182** (2018), 179–205. MR 3703936

**10.** D. Mirimanoff, *L'équation indéterminée $x^\ell + y^\ell + z^\ell = 0$ et le critérium de Kummer*, J. Reine Angew. Math. **128** (1905), 45–68. MR 1580644

**11.** P. Ribenboim, *13 lectures on Fermat's last theorem*, Springer-Verlag, New York, 1979. MR 551363 (81f:10023)


https://doi.org/10.1017/S0017089520000026 Published online by Cambridge University Press