The irreducibility of polynomials related to work of Heim, Luca and Neuhauser

by

JOSEPH C FOSTER (New York, NY) and
JEREMIAH SOUTHWICK (Columbia, SC)

In memory of Professor Andrzej Schinzel

1. Introduction. In [7], Heim and Neuhauser were interested in the family of polynomials defined with initial condition \( P_0(X) = 1 \) and recursion

\[
P_n(X) = \frac{X}{n} \sum_{k=1}^{n} \sigma(k)P_{n-k}(X)
\]

for \( n \geq 1 \), where \( \sigma(n) \) is the sum of divisors function. These polynomials arise as Fourier coefficients of powers of the Dedekind eta functions, as shown by Newman in [11]. In [6], Heim, Luca and Neuhauser generalised the recurrence relation in (1.1) by replacing \( \sigma(n) \) with other arithmetic functions. Namely, they studied the following

**Definition 1.1.** Let \( g(n) \) be an arithmetic function. Define a family of polynomials \( P^n_g(X) \) associated with \( g \) by \( P^n_0(X) := 1 \) and

\[
P^n_g(X) = \frac{X}{n} \sum_{k=1}^{n} g(k)P_{n-k}(X).
\]

In particular, they looked at the coefficients of \( X \) in \( P^n_g(X) \) for \( g(n) = n \) and \( g(n) = n^2 \) as these functions provide bounds on \( \sigma(n) \). They found explicit formulas for the coefficients and concluded

\[
P^n(X) = X \sum_{k=0}^{n-1} \frac{1}{(k+1)!} \binom{n-1}{k} X^k
\]

2020 Mathematics Subject Classification: Primary 11R09; Secondary 11B83, 11C08.

Key words and phrases: irreducible polynomial, Newton polygons.

Received 12 February 2023.
Published online 25 September 2023.

DOI: 10.4064/aa230212-10-7
\[ P^{n^2}_n(X) = X \sum_{k=0}^{n-1} \frac{1}{(k+1)!} \left( \frac{n+k}{2k+1} \right)^k \. \]

In [6], Heim, Lucas and Neuhauser looked further at these polynomials. One of the results they obtained was the irreducibility of the polynomials

\[ \tilde{P}^n_n(X) = \frac{n!}{X} P^n_n(X) = \sum_{k=0}^{n-1} \frac{n!}{(k+1)!} \left( \frac{n-1}{k} \right) X^k. \]

They also conjectured the irreducibility of the polynomials

\[ \tilde{P}^{n^2}_n(X) = \frac{n!}{X} P^{n^2}_n(X) = \sum_{k=0}^{n-1} \frac{n!}{(k+1)!} \left( \frac{n+k}{2k+1} \right) X^k, \]

a result that was proven by the authors of this paper and Juillerat [4].

The goal of this paper is to look at the irreducibility of the polynomials that arise when \( g(n) = n^t \) for any positive integer \( t \). To obtain these polynomials we modify the derivation of the polynomials in [7] which begins with the identity

\[ \sum_{n=0}^{\infty} P^{n^t}_n(X) q^n = \exp \left( X \sum_{n=1}^{\infty} \frac{n^t}{n} q^n \right). \tag{1.2} \]

We expand the right-hand side of (1.2) and manipulate it to compare formally the coefficients of the different powers of \( q \). We have

\[
\begin{align*}
\exp \left( X \sum_{n=1}^{\infty} \frac{n^t}{n} q^n \right) &= 1 + \sum_{k=1}^{\infty} \frac{1}{k!} X^k \left( \sum_{n=1}^{\infty} n^{t-1} q^n \right)^k \\
&= 1 + \sum_{k=1}^{\infty} \frac{1}{k!} X^k \left( \sum_{m_1=1}^{\infty} \ldots \sum_{m_k=1}^{\infty} m_1^{t-1} \ldots m_k^{t-1} q^{m_1+\ldots+m_k} \right) \\
&= 1 + \sum_{n=1}^{\infty} \sum_{k=1}^{n} \frac{1}{k!} X^k \left( \sum_{m_1+\ldots+m_k=n} m_1^{t-1} \ldots m_k^{t-1} \right) q^n,
\end{align*}
\]

where, in the innermost sum, the \( m_i \) are positive integers. Thus for \( n \geq 1 \) we obtain

\[ P^{n^t}_n(X) = \sum_{k=1}^{n} \frac{1}{k!} \left( \sum_{m_1+\ldots+m_k=n} m_1^{t-1} \ldots m_k^{t-1} \right) X^k. \]

For \( 1 \leq k \leq n \) and \( t \) a positive integer, define

\[ S(k | n, t) = \sum_{m_1+\ldots+m_k=n} m_1^t \ldots m_k^t. \]

Consequently, the goal of this paper is to prove the following
Theorem 1.2. The polynomials

\[ f(x \mid n, t) = \sum_{k=1}^{n} \frac{n!}{k!} S(k \mid n, t) x^{k-1} \]  

are irreducible for all integers \( n \geq 2 \) and \( t \geq 1 \).

Here, we note that \( P_{n}^{t}(X) = (X/n!) f(X \mid n, t - 1) \). The proof of Theorem 1.2 will follow similarly to that of the main result in [4]. In Section 2, we define Newton polygons along with stating a theorem of Dumas [1], and we list several results regarding factorials and binomial coefficients. Section 3 is dedicated to studying the expressions \( S(k \mid n, t) \) so that we can construct the Newton polygons of \( f(x \mid n, t) \) in Section 4. We bring everything together to prove Theorem 1.2 in Section 5.

2. Preliminary material. We first introduce the notion of Newton polygons. Let \( f(x) = \sum_{j=0}^{r} a_{j} x^{j} \in \mathbb{Z}[x] \) with \( a_{0} a_{r} \neq 0 \) and fix a prime \( p \). For an integer \( m \neq 0 \), denote by \( \nu_{p}(m) \) the \( p \)-adic valuation of \( m \), that is, the exponent in the largest power of \( p \) dividing \( m \). Let \( S \) be the set of lattice points \((j, \nu_{p}(a_{r-j}))\) for \( 0 \leq j \leq r \) with \( a_{r-j} \neq 0 \). The Newton polygon of \( f(x) \) with respect to the prime \( p \) is the polygonal path along the lower convex hull of these points from \((0, \nu_{p}(a_{r}))\) to \((r, \nu_{p}(a_{0}))\). The endpoints of every edge belong to the set \( S \), and the slopes of the edges strictly increase as we move from left to right along the Newton polygon.

Newton polygons hold a wealth of information regarding the irreducibility of a polynomial. The main result we use regarding Newton polygons is due to Dumas [11, 12] and relates the Newton polygons of two polynomials to the Newton polygon of their product.

Theorem 2.1. Let \( g(x) \) and \( h(x) \) be in \( \mathbb{Z}[x] \) with \( g(0) h(0) \neq 0 \), and let \( p \) be a prime. Let \( k \) be a non-negative integer such that \( p^{k} \) divides the leading coefficient of \( g(x) h(x) \) but \( p^{k+1} \) does not. Then the edges of the Newton polygon for \( g(x) h(x) \) with respect to \( p \) can be formed by constructing a polygonal path beginning at \((0, k)\) and using translates of the edges in the Newton polygons for \( g(x) \) and \( h(x) \) with respect to the prime \( p \), using exactly one translate for each edge of the Newton polygons for \( g(x) \) and \( h(x) \). Necessarily, the translated edges are translated in such a way as to form a polygonal path with the slopes of the edges increasing from left to right.

We prove Theorem 1.2 by explicitly constructing the Newton polygons for \( f(x \mid n, t) \) for each prime \( p \) dividing \( n - 1 \). To do this we make use of three lemmas regarding binomial coefficients, factorials and their \( p \)-adic valuation. The first is a classical result of Legendre [9].
Lemma 2.2. Let \( n \) be a positive integer, and let \( p \) be a prime. Let \( s_p(n) \) denote the sum of the base \( p \) digits of \( n \). Then

\[
\nu_p(n!) = \frac{n - s_p(n)}{p - 1}.
\]

Lemma 2.2 implies the following result due to Kummer [8].

Lemma 2.3. Let \( n \) and \( j \) be integers with \( 0 \leq j \leq n \). Then

\[
\nu_p\left(\binom{n}{j}\right) = s_p(j) + s_p(n - j) - s_p(n) - 1.
\]

Equivalently, \( \nu_p\left(\binom{n}{j}\right) \) is the number of borrows encountered when subtracting \( j \) from \( n \) in base \( p \).

We also note Lucas’s binomial theorem [10].

Lemma 2.4. Let \( n \geq j \) be non-negative integers. In base \( p \), write \( n = a_r p^r + \cdots + a_1 p + a_0 \) and \( j = j_r p^r + \cdots + j_1 p + j_0 \) where \( 0 \leq a_i, j_i \leq p - 1 \) for each \( i \in \{0, 1, \ldots, r\} \), and \( a_r \neq 0 \). Then

\[
\binom{n}{j} \equiv \binom{a_r}{j_r} \cdots \binom{a_1}{j_1} \binom{a_0}{j_0} \pmod{p}.
\]

3. An explicit formulation of the coefficients. To construct the Newton polygons of \( f(x \mid n, t) \) we will require a clearer understanding of the numbers \( S(k \mid n, t) \). Specifically, we will want to know enough about \( S(k \mid n, t) \) so that we can talk about its \( p \)-adic valuation with respect to different primes.

Firstly, observe that

\[
S(k \mid n, t) = \sum_{m_1 + \cdots + m_k = n} m_1^t \cdots m_k^t = [x^n]\left((x + 2tx^2 + 3tx^3 + 4tx^4 + \cdots)^k\right),
\]

where \( [x^n](h(x)) \) denotes the coefficient of \( x^n \) in the power series \( h(x) \).

Secondly, taking \( |x| < 1 \), recall

\[
\frac{1}{1 - x} = 1 + x + x^2 + x^3 + x^4 + \cdots,
\]

and observe that

\[
\frac{d}{dx}\left(\frac{1}{1 - x}\right) = x(1 + 2x + 3x^2 + \cdots) = x + 2x^2 + 3x^3 + \cdots.
\]

Iterating this pair of operations \( t \) times, we obtain

\[
\underbrace{x \frac{d}{dx}\left(\cdots \left(x \frac{d}{dx}\left(\frac{1}{1 - x}\right)\right)\cdots\right)}_{t \text{ times}} = x + 2^tx^2 + 3^tx^3 + 4^tx^4 + \cdots.
\]

For ease of notation, let \( D(\cdot) := x(d/dx)(\cdot) \). Then

\[
S(k \mid n, t) = [x^n]\left((D^t((1 - x)^{-1}))^k\right).
\]
To study the numbers $S(k \mid n, t)$ we start by studying the sequence $\{D^t(1/(1 - x))\}_{t \in \mathbb{N}}$. An induction argument shows that $D^t(1/(1 - x))$ is $x$ times a polynomial of degree $t - 1$ divided by $(1 - x)^{t+1}$. Define $A_{t,j}$ by

\begin{equation}
D^t \left( \frac{1}{1 - x} \right) = \frac{x \sum_{j=0}^{t-1} A_{t,j} x^j}{(1 - x)^{t+1}}.
\end{equation}

Then, for any $t \geq 1$, we deduce

\[
\frac{d}{dx} \left( D^t \left( \frac{1}{1 - x} \right) \right) = \frac{d}{dx} \left( \frac{x \sum_{j=0}^{t-1} A_{t,j} x^j}{(1 - x)^{t+1}} \right)
\]

\[
= \frac{(1 - x)^{t+1} \sum_{j=0}^{t-1} (j + 1) A_{t,j} x^j + (t + 1)(1 - x)^t \sum_{j=1}^{t} A_{t,j-1} x^j}{(1 - x)^{2t+2}}
\]

\[
= \frac{\sum_{j=0}^{t-1} (j + 1) A_{t,j} x^j - \sum_{j=1}^{t} j A_{t,j-1} x^j + (t + 1) \sum_{j=1}^{t} A_{t,j-1} x^j}{(1 - x)^{t+2}}
\]

\[
= \frac{A_{t,0} + \sum_{j=1}^{t-1} [(j + 1) A_{t,j} + (t - j + 1) A_{t,j-1}] x^j + A_{t,t-1} x^t}{(1 - x)^{t+2}}.
\]

Observe that $A_{1,0} = 1$ and from the above, for $0 \leq j \leq t$, we have

\begin{equation}
A_{t+1,j} = \begin{cases} 
A_{t,0} & \text{if } j = 0, \\
(j + 1) A_{t,j} + (t - j + 1) A_{t,j-1} & \text{if } 1 \leq j \leq t - 1, \\
A_{t,t-1} & \text{if } j = t.
\end{cases}
\end{equation}

The numbers $A_{t,j}$ are the so-called Eulerian numbers (see [2, 3, 5, 13]). We will make use of the following identities associated with the Eulerian numbers:

\begin{equation}
A_{t,j} = \sum_{i=0}^{m} (-1)^i \binom{t+1}{i} (j + 1 - i)^t,
\end{equation}

\begin{equation}
x^t = \sum_{m=0}^{t-1} A_{t,m} \binom{x+m}{t},
\end{equation}

\begin{equation}
A_{t,m} = A_{t,t-1-m}.
\end{equation}

Combining [3.1] and [3.2] yields

\begin{equation}
S(k \mid n, t) = [x^n] \left( \frac{x \sum_{j=0}^{t-1} A_{t,j} x^j}{(1 - x)^{t+1}} \right)^k = [x^{n-k}] \left( \frac{\sum_{j=0}^{t-1} A_{t,j} x^j}{(1 - x)^{k(t+1)}} \right)^k.
\end{equation}

Substituting [3.4] into the right-hand side of (3.7) and expanding with multinomial coefficients yields the following

**Lemma 3.1.** The value $S(k \mid n, t)$ is the coefficient of $x^{n-k}$ in the expansion of
\[
\sum_{k_0+\ldots+k_{t-1}=k} \binom{k}{k_0, \ldots, k_{t-1}} \left( \prod_{i=0}^{t-1} A_{t,i}^{k_i} \right) x^{\sum_{i=0}^{t-1} i k_i} \sum_{j=0}^{\infty} \left( j + (t+1)k - 1 \right) x^j,
\]

where \(k_0, k_1, \ldots, k_{t-1}\) represent non-negative integers.

4. Constructing the Newton polygons. The remainder of this paper follows the basic idea discussed in [4]. That is, we will first explicitly construct the Newton polygons for \(f(x \mid n, t)\) with respect to each prime \(p \mid (n-1)\) and then apply Theorem 2.1 to show that any factor of \(f(x \mid n, t)\) has degree at least \(n-1\). We start by introducing some notation.

Let \(v = \nu_p(n-1)\) and \(u = \lfloor \log_p(n-1) \rfloor - v\). Note that since \(p \mid (n-1)\), we have \(v \geq 1\). Then

\[
(4.1) \quad n - 1 = p^v \sum_{j=0}^{u} a_j p^j, \quad \text{where } a_u, a_0 \geq 1,
\]

is the base \(p\) expansion of \(n - 1\). For each \(J \in \{0, 1, \ldots, u\}\), we denote by \(n_J\) the \(p^{v+J}\)th truncation of \(n - 1\) in base \(p\). That is,

\[
(4.2) \quad n_J = p^v \sum_{j=0}^{J} a_j p^j.
\]

Let \(n_{-1} = 0\). It is useful to note at this point that when \(J = u\), we get \(n - n_J = 1\), and more generally, when \(J \in \{-1, 0, \ldots, u\}\), we have

\[
(4.3) \quad n - n_J = 1 + p^v \sum_{j=J+1}^{u} a_j p^j.
\]

We prove the following

**Theorem 4.1.** Fix integers \(n \geq 3\) and \(t \geq 1\). Let \(f(x \mid n, t)\) as in (1.3). Let \(p\) be a prime dividing \(n - 1\), and let

\[
n - 1 = p^v \sum_{j=0}^{u} a_j p^j
\]

be the \(p\)-ary expansion of \(n - 1\) as in (4.1). Then the vertices of the Newton polygon for \(f(x \mid n, t)\) with respect to \(p\) are precisely the points in the set

\[
(4.4) \quad \{(0, 0)\} \cup \left\{ \left( \sum_{j=0}^{J} a_j p^{v+j}, \sum_{j=0}^{J} a_j p^{v+j} - 1 \right) \left/ \left( \sum_{j=0}^{J} a_j p^{v+j} - 1 \right) \right\} \mid J \in \{0, 1, \ldots, u\} \right\}.
\]

To prove Theorem 4.1 it suffices to show each of the following:

1. The Newton polygon for \(f(x \mid n, t)\) with respect to \(p\) is the lower convex hull of the points in (4.4).
The irreducibility of polynomials

(2) The slopes of the edges joining the successive pairs of points in (4.4) are strictly increasing from left to right.

To do this we will first establish two lemmas.

**Lemma 4.2.** Let \( p \mid (n-1) \). Then for each \( J \in \{0, \ldots, u\} \), we have

\[
\nu_p(S(n-n_J \mid n, t)) = 0.
\]

**Proof.** Since \( n-(n-n_J) = n_J \), Lemma 3.1 implies that \( S(n-n_J \mid n, t) \) is the coefficient of \( x^{n_J} \) in the expansion of

\[
(4.5) \quad \sum_{k_0 + \cdots + k_{t-1} = n-n_J} \binom{n-n_J}{k_0, \ldots, k_{t-1}} \left( \prod_{i=0}^{t-1} A_{t,i}^{k_i} \right) x^\sum_{i=0}^{t-1} ik_i
\]

multiplied by

\[
\sum_{j=0}^{\infty} \left( \frac{j + (t+1)(n-n_J) - 1}{(t+1)(n-n_J) - 1} \right) x^j.
\]

We first focus our attention on the left factor in (4.5). We fix \( 0 < i_0 \leq t-1 \) and derive conditions on \( k_{i_0} \) necessary for a given term in (4.5) not to contribute to \( S(n-n_J \mid n, t) \). In particular, if \( k_{i_0} \geq p^{v+J+1} \), then by (4.2) we have

\[
\sum_{i=0}^{t-1} ik_i \geq i_0 k_{i_0} \geq p^{v+J+1} > n_J.
\]

Thus no terms in (4.5) with such values for \( k_{i_0} \) would contribute to \( S(n-n_J \mid n, t) \). So for all \( i \in \{1, \ldots, t-1\} \), we need only consider terms from (4.5) with \( k_{i_0} < p^{v+J+1} \).

Now we fix more generally \( 0 \leq i_0 \leq t-1 \). By considering (4.3) we see for \( J \in \{0, \ldots, u-1\} \) that if \( k_{i_0} \not\equiv 0, 1 \pmod{p^{v+J+1}} \), then there will be at least one borrow when subtracting \( k_{i_0} \) from \( n-n_J \) in base \( p \). Hence, by Lemma 2.3, we obtain \( p \mid \binom{n-n_J}{k_{i_0}} \), implying

\[
p \mid \left( \binom{n-n_J}{k_0, \ldots, k_{t-1}} \right) = \binom{n-n_J}{k_{i_0}} \left( \binom{n-n_J-k_{i_0}}{k_0, \ldots, k_{i_0-1}, k_{i_0+1}, \ldots, k_{t-1}} \right).
\]

Thus, to determine \( S(n-n_J \mid n, t) \) modulo \( p \), we need only consider terms in (4.5) with \( k_0 \equiv 0, 1 \pmod{p^{v+J+1}} \) and \( k_i = 0, 1 \) for each \( i \in \{1, \ldots, t-1\} \).

With \( i \in \{1, \ldots, t-1\} \) and \( k_i \) as in the sum in (4.5), let \( z \) be the number of such \( i \) with \( k_i = 1 \). Then \( k_0 = n-n_J - z \equiv 1 - z \pmod{p^{v+J+1}} \), where the congruence comes from (4.3). Since \( k_0 \equiv 0, 1 \pmod{p^{v+J+1}} \), we must then have

\[
z \equiv 1, 0 \pmod{p^{v+J+1}}.
\]
If $z \geq p^{v+J+1}$, then we would have
\[
\sum_{i=0}^{t-1} i k_i = \sum_{1 \leq i \leq t-1, k_i=1} i \geq \sum_{1 \leq i \leq t-1, k_i=1} 1 = z \geq p^{v+J+1} > n_J.
\]
This means we only need to consider $z = 1, 0$. Hence, since $A_{t,0} = 1$, we use (4.3) to deduce for each $J \in \{0, \ldots, u\}$ that
\[
(4.6) \quad S(n - n_J \mid n, t) \equiv \left(\frac{n_J + (t+1)(n - n_J) - 1}{n_J}\right)
+ (n - n_J) \sum_{j=1}^{t-1} A_{t,j} \left(\frac{n_J - j + (t+1)(n - n_J) - 1}{n_J - j}\right)
\equiv \sum_{j=0}^{t-1} A_{t,j} \left(\frac{n_J - j + (t+1)(n - n_J) - 1}{n_J - j}\right) (\text{mod } p).
\]
Rewriting (4.6) yields
\[
S(n - n_J \mid n, t) \equiv \sum_{j=0}^{t-1} A_{t,j} \left(\frac{n_J - j + (t+1)(n - n_J) - 1}{n_J - j}\right) (\text{mod } p).
\]
Since $(t+1)(n - 1 - n_J) \equiv 0 \pmod{p^{v+J+1}}$, and $n_J - j < p^{v+J+1}$ for $0 \leq j \leq t-1$, any borrows in the subtraction $(n_J - j + (t+1)(n - 1 - n_J) + t) - (n_J - j)$ in base $p$ will come from the subtraction $(n_J - j + t) - (n_J - j)$ in base $p$.

We can use these facts to simplify $S(n - n_J \mid n, t)$ further. Via the division algorithm, we write $n_J - j + t = q \cdot p^{v+J+1} + r$ where $0 \leq r < p^{v+J+1}$. Then the base $p$ expansion of $n_J - j + (t+1)(n - 1 - n_J) + t$ has its digits in the $p^{v+J+1}$-place and higher arising from $(t+1)(n - 1 - n_J) + q \cdot p^{v+J+1}$, while the lower digits arise from $r$. Thus, we can use Lemma 2.4 to obtain
\[
\left(\frac{n_J - j + (t+1)(n - 1 - n_J) + t}{n_J - j}\right)
\equiv \left(\frac{(t+1)(n - 1 - n_J)/p^{v+J+1} + q}{n_J - j}\right) \left(\frac{r}{n_J - j}\right)
\equiv \left(\frac{q}{0}\right) \left(\frac{r}{n_J - j}\right) \equiv \left(\frac{n_J - j + t}{n_J - j}\right) (\text{mod } p).
\]
Substituting this simplification into $S(n - n_J \mid n, t)$, we obtain
\[
S(n - n_J \mid n, t) \equiv \sum_{j=0}^{t-1} A_{t,j} \left(\frac{n_J - j + t}{n_J - j}\right) (\text{mod } p).
\]
Using the symmetry of binomial coefficients, we have
\[ S(n - n_J | n, t) \equiv \sum_{j=0}^{t-1} A_{t,j} \binom{n_J - j + t}{t} \equiv (n_J + 1)^t \pmod{p}, \]
where the second equivalence comes from (3.5) and (3.6). Recalling that \( n_J \) is divisible by \( p^v \), we see \( S(n - n_J | n, t) \equiv 1 \pmod{p} \) so that the lemma follows.

While Lemma 4.2 will allow us to find candidates for the vertices on the Newton polygon of \( f(x | n, t) \), we will use the following lemma to show that no other vertices can appear in the Newton polygon.

**Lemma 4.3.** Let \( p \mid (n - 1) \). If \( m \equiv n \pmod{p} \), then
\[ \nu_p(S(n - m | n, t)) > 0. \]

**Proof.** By Lemma 3.1, we see that \( S(n - m | n, t) \) is the coefficient of \( x^{n-(n-m)} = x^m \) in the expansion of
\[ \sum_{k_0 + \cdots + k_{t-1} = n-m} \binom{n-m}{k_0, \ldots, k_{t-1}} (\prod_{i=0}^{t-1} A_{t,i}) \sum_{i=0}^{t-1} i k_i \]
multiplied by
\[ \sum_{j=0}^{\infty} \binom{j + (t + 1)(n - m) - 1}{(t + 1)(n - m) - 1} x^j. \]

We fix \( 0 \leq i_0 \leq t - 1 \) and consider the \( k_{i_0} \) appearing in the left factor above. Since \( m \equiv n \pmod{p} \), we have \( p \mid (n - m) \). If \( p \nmid k_{i_0} \), then we can rewrite the multinomial coefficient and use Lemma 2.3 to obtain
\[ \binom{n-m}{k_0, \ldots, k_{t-1}} = \binom{n-m}{k_{i_0}, \ldots, k_{i_0-1}, k_{i_0+1}, \ldots, k_{t-1}} \equiv 0 \pmod{p}, \]
since there will be a carry when subtracting \( k_{i_0} \) from \( n - m \) in base \( p \). Thus the only non-zero terms in
\[ \sum_{k_0 + \cdots + k_{t-1} = n-m} \binom{n-m}{k_0, \ldots, k_{t-1}} (\prod_{i=0}^{t-1} A_{t,i}) \sum_{i=0}^{t-1} i k_i, \]
when considered modulo \( p \), are those where for each \( i \in \{0, \ldots, t-1\} \) there are non-negative integers \( k'_i \) such that \( k_i = pk'_i \). That is, reducing \( S(n - m | n, t) \pmod{p} \), we need only consider the coefficient of \( x^m \) arising from the multiplication of
\[ \sum_{pk'_{i_0} + \cdots + pk'_{t-1} = n-m} \binom{n-m}{pk'_{i_0}, \ldots, pk'_{t-1}} (\prod_{i=0}^{t-1} A_{t,i}^{p k'_i}) \sum_{i=0}^{t-1} i pk'_i \]
by
\[
\sum_{j=0}^{\infty} \binom{j + (t + 1)(n - m) - 1}{(t + 1)(n - m) - 1} x^j.
\]

For each term in the first sum, in order to get a contribution to the coefficient of \(x^m\) in the product, we want to consider
\[
j = m - \sum_{i=0}^{t-1} ipk'_i
\]
in the second sum.

We now turn our attention to the binomial coefficients
\[
\binom{j + (t + 1)(n - m) - 1}{(t + 1)(n - m) - 1} = \binom{m - \sum_{i=0}^{t-1} ipk'_i + (t + 1)(n - m) - 1}{(t + 1)(n - m) - 1}.
\]
Recall \(m \equiv n \equiv 1 \pmod{p}\), so
\[
m - \sum_{i=0}^{t-1} ipk'_i + (t + 1)(n - m) - 1 \equiv 0 \pmod{p}
\]
and
\[
(t + 1)(n - m) - 1 \equiv p - 1 \pmod{p}.
\]
Thus, Lemma 2.3 implies that
\[
\binom{m - \sum_{i=0}^{t-1} ipk'_i + (t + 1)(n - m) - 1}{(t + 1)(n - m) - 1} \equiv 0 \pmod{p}.
\]
Hence, \(S(n - m \mid n, t) \equiv 0 \pmod{p}\) since each term contributing to the coefficient of \(x^m\) in the product above is divisible by \(p\). The lemma follows.

**Proof of Theorem 4.1.** Recall it suffices to show each of the following:

1. The Newton polygon for \(f(x \mid n, t)\) with respect to \(p\) is the lower convex hull of the points in (4.4).
2. The slopes of the edges joining the successive pairs of points in (4.4) are strictly increasing from left to right.

Fix integers \(n \geq 3\), \(t \geq 1\) and a prime \(p\) dividing \(n - 1\). Starting with (1) for \(0 \leq j \leq n - 1\), set
\[
c_j = \frac{n!}{j!} S(j \mid n, t) = (n - j)! \binom{n}{n - j} S(j \mid n, t).
\]
Thus \(f(x \mid n, t) = \sum_{j=1}^{n} c_j x^{j-1}\). For \(J \in \{0, \ldots, u\}\) define \(n_J\) as in (4.2), with \(n_{-1} = 0\). Note that since \(f(x \mid n, t)\) is monic, \(\nu_p(c_n) = \nu_p(1) = 0\), meaning \((0, \nu_p(c_n)) = (0, 0)\) is on the Newton polygon with respect to \(p\).
Next, we show for $J \in \{0, 1, \ldots, u\}$ that
\begin{equation}
\nu_p(c_{n-n,J}) = \frac{1}{p-1} \sum_{j=0}^{J} a_j(p^{v+j} - 1).
\end{equation}

Using the definition of $\nu_p(\cdot)$, we see that
\begin{equation}
\nu_p(c_{n-n,J}) = \nu_p(nJ!) + \nu_p\left(\binom{n}{nJ}\right) + \nu_p(S(n-nJ \mid n, t)).
\end{equation}

Since $n-n_J$ requires no carries in base $p$, so, applying Lemmas 2.2, 2.3 and 4.2 to the respective terms in (4.8), we have
\begin{equation}
\nu_p(c_{n-n,J}) = \frac{n_J - s_p(n_J)}{p-1} + 0 + 0 = \frac{1}{p-1} \sum_{j=0}^{J} a_j(p^{v+j} - 1).
\end{equation}

Thus, we see (4.7) holds, and the set (4.4) is precisely the set
\begin{equation}
\{(nJ, \nu_p(c_{n-n,J})) \mid J \in \{-1, 0, \ldots, u\}\}.
\end{equation}

To prove (1) we must show that all points in the set
\begin{equation}
\{(j, \nu_p(c_{n-j})) \mid j \in \{0, 1, \ldots, n-1\}\}
\end{equation}
lie on or above the lines joining successive points in (4.9). It is clear that the points in (4.9) lie on said lines, so consider a point $(m, \nu_p(c_{n-m}))$ not belonging to (4.9).

If $n_J < m < n_{J+1}$ for some $J \in \{-1, 0, \ldots, u-1\}$, then it suffices to show
\begin{equation}
\frac{\nu_p(c_{n-m}) - \nu_p(c_{n-n,J})}{m-n_J} \geq \frac{\nu_p(c_{n-n,J+1}) - \nu_p(c_{n-n,J})}{n_{J+1} - n_J}.
\end{equation}

Using the definition of $\nu_p(\cdot)$ once more with (4.7), we deduce that the inequality in (4.10) is equivalent to
\begin{equation}
\frac{\nu_p(m!) + \nu_p(\binom{n}{m}) + \nu_p(S(n-m \mid n, t)) - (n_J - s_p(n_J))/(p-1)}{m-n_J} \geq \frac{p^{v+J+1} - 1}{(p-1)p^{v+J+1}}.
\end{equation}

We note from (4.3) and $v \geq 1$ that $s_p(n) - s_p(n_J) = s_p(n-n_J)$. Using this observation along with Lemmas 2.2 and 2.3, we multiply both sides by $p-1$ to transform (4.11) into
\begin{equation}
\frac{(m-n_J) + (s_p(n-m) - s_p(n-n_J)) + (p-1)\nu_p(S(n-m \mid n, t))}{m-n_J} \geq \frac{p^{v+J+1} - 1}{p^{v+J+1}}.
\end{equation}
Subtracting 1 and then multiplying both sides by \( m - n_J \) yields
\[
s_p(n - m) - s_p(n - n_J) + (p - 1)\nu_p(S(n - m \mid n, t)) \geq \frac{m - n_J}{p^{v+J+1}}. \tag{4.12}
\]
From [4.3], we have
\[
n - n_J = n - 1 - n_J + 1 = p^v \sum_{j=J+1}^u a_j p^j + 1,
\]
so
\[
s_p(n - n_J) = 1 + \sum_{j=J+1}^u a_j. \tag{4.13}
\]
Recall \( n_J < m < n_{J+1} \). In the equations that follow we interpret a sum from \( j = u + 1 \) to \( j = u \) as 0, which arises when \( J = u - 1 \). Then we can write
\[
n - m = (n - 1 - n_{J+1}) + (n_{J+1} + 1 - m)
= p^v \sum_{j=J+2}^u a_j p^j + \sum_{j \in T} \epsilon_j p^j,
\]
where \( T \subseteq \{0, 1, \ldots J + v + 1\} \) is a non-empty set and \( \epsilon_j \in \{1, \ldots, p - 1\} \) for each \( j \). Thus, we obtain
\[
s_p(n - m) = \sum_{j=J+2}^u a_j + \sum_{j \in T} \epsilon_j. \tag{4.15}
\]
Further, we can write
\[
n - m = (n - 1 - n_J) + (n_J + 1 - m)
= p^v \sum_{j=J+1}^u a_j p^j + n_J + 1 - m.
\]
Setting the right-hand sides of [4.14] and [4.16] equal and solving for \( n_J - m \) gives
\[
n_J - m = \sum_{j \in T} \epsilon_j p^j - a_{J+1} p^{v+J+1} - 1. \tag{4.17}
\]
Substituting (4.13), (4.15) and (4.17) into (4.12) yields
\[
\sum_{j \in T} \epsilon_j - a_{J+1} - 1 + (p - 1)\nu_p(S(n - m \mid n, t))
\geq \sum_{j \in T} \frac{\epsilon_j p^j - a_{J+1} p^{v+J+1} - 1}{p^{v+J+1}}.
\]
Rearranging the above gives
\[
\sum_{j \in T} \epsilon_j (1 - p^{j-v-J-1}) - 1 + (p - 1)\nu_p(S(n - m \mid n, t)) \geq -p^{-v-J-1}. \tag{4.18}
\]
Recall $T \neq \emptyset$. Observe that if $\nu_p(S(n - m \mid n, t)) > 0$, then the left-hand side of (4.18) is positive, and so the inequality holds. Alternatively, the contrapositive of Lemma 4.3 tells us that if $\nu_p(S(n - m \mid n, t)) = 0$, then $m \not\equiv n \pmod{p}$, implying $0 \in T$ so that $\epsilon_0 \geq 1$. This allows us to simplify the left-hand side of (4.18) and obtain

$$
\sum_{j \in T} \epsilon_j(1 - p^j - v - J - 1) - 1 \geq \epsilon_0(1 - p^v - J - 1) - 1 \\
\geq (1 - p^v - J - 1) - 1 = p^{-v} - J - 1.
$$

Thus, (4.18) and the equivalent (4.10) hold. This completes the proof of (1).

For (2), let $J$ be such that $n J \neq n J + 1$. Then

$$
\frac{\nu_p(c_{n-n J+1}) - \nu_p(c_{n-n J})}{n_{J+1} - n J} = \frac{a_{J+1}(p^{v+J+1} - 1)}{(p - 1)a_{J+1}p^{v+J+1}} = \frac{1}{p - 1}(1 - \frac{1}{p^v + J + 1}).
$$

Since the right-hand side of (4.19) increases as $J$ increases, we deduce that (2) holds. This completes the proof of the Theorem 4.1.

5. Proof of Theorem 1.2. We now have what we need to prove Theorem 1.2, namely

**Theorem 1.2.** The polynomials

$$
f(x \mid n, t) = \sum_{k=1}^{n} \frac{n!}{k!} S(k \mid n, t)x^{k-1}
$$

are irreducible for all integers $n \geq 2$ and $t \geq 1$.

**Proof.** When $n = 2$, we have $f(x \mid 2, t) = x + 2^t$, which is irreducible. For $n \geq 3$, let $p$ be a prime dividing $n - 1$ and adopt the notation of Section 4. From the proof of Theorem 4.1, the slope of the line segment joining two successive points in (4.4) is of the form

$$
\frac{1}{p - 1} \left(1 - \frac{1}{p^{v+J+1}}\right) = \frac{p^{v+J+1} - 1}{(p - 1)p^{v+J+1}}
$$

for $J \in \{-1, 0, 1, \ldots, u\}$. Observe that when this last fraction is reduced, the denominator is $p^{v+J+1}$. This implies that for a segment with this slope, the horizontal distance between the consecutive lattice points is $p^{v+J+1}$. In particular, from Theorem 4.1, the smallest horizontal distance between any two consecutive lattice points on the Newton polygon of $f(x \mid n, t)$ with respect to $p$ is $p^v$, and so the horizontal distance between every pair of consecutive lattice points is divisible by $p^v$. This is true for every prime power $p^v$ dividing $n-1$. Thus, any irreducible factor of $f(x \mid n, t)$ has degree divisible by $n - 1$. Since the degree of $f(x \mid n, t)$ is $n - 1$, the proof is complete.
References


