AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **89(1)** (2024), Pages 116–136

Congruences for Sheffer sequences

Grzegorz Serafin

Faculty of Pure and Applied Mathematics
Wrocław University of Science and Technology
Ul. Wybrzeże Wyspiańskiego 27, Wrocław
Poland
grzegorz.serafin@pwr.edu.pl

Abstract

We provide necessary and sufficient conditions for general Sheffer polynomials $P_n(x)$ to satisfy the Touchard congruence $P_{n+p}(x) \equiv x^p P_n(x) + P_{n+1}(x) \pmod{p\mathbb{Z}[x]}$ and its generalizations, or to satisfy the elegant congruence $P_{n+p}(x) \equiv P_p(x)P_n(x) \pmod{p\mathbb{Z}[x]}$, for a prime p, that is a feature of e.g. factorial polynomials. Eventually, we examine periodicity of the related number sequences modulo a prime number. Some examples are provided as well. The obtained congruences might be understood as a wide extension of divisibility properties of the Touchard (Bell) polynomials and Stirling numbers of both kinds. However, despite the high generality of the results, we employ relatively simple methods.

1 Introduction

In this article, we investigate the divisibility properties of Sheffer sequences, which constitute a wide class of polynomials, including e.g. the Touchard (Bell), factorial, Hermite, Bernoulli, Laguerre and derangement polynomials, and contains a subclass of Appell polynomials. Furthermore, (finite) moments of Lévy processes are Sheffer polynomials of the time parameter. For two formal power series $f(t) = \sum_{n=0}^{\infty} f_n t^n/n!$, $g(t) = \sum_{n=0}^{\infty} g_n t^n/n!$ with $f_0 = 0$, $f_1, g_0 \neq 0$, we define the Sheffer sequence as the sequence of polynomials

$$P_n(x) = \sum_{k=0}^{n} S(n,k)x^k$$

given by its exponential generating function [34]

$$\mathbf{G}(t,x) := \sum_{n=0}^{\infty} P_n(x)\frac{t^n}{n!} = g(t)e^{xf(t)}. \tag{1.1}$$

ISSN: 2202-3518 ©The author(s). Released under the CC BY 4.0 International License

Fixing $x = 1$, we obtain related number sequences $(P_n)_{n\geq 0} := (P_n(1))_{n\geq 0}$. Additionally, given our focus on divisibility properties, we assume f_n and g_n to be integers. In fact p-adic integers might be considered as well.

One of the most classical results for these kind of polynomials is the Touchard congruence (see [38, 28, 14, 11]), which states that

$$B_{n+p}(x) \equiv x^p B_n(x) + B_{n+1}(x) \pmod{p\mathbb{Z}[x]}, \tag{1.2}$$

where p is any prime, $n \in \mathbb{N}_0 = \{0, 1, 2, 3, \ldots\}$ and $B_n(x) = \sum_{k=0}^{n} \left\{ {n \atop k} \right\} x^k$ is the Touchard (called also Bell) polynomial arising from (1.1) with $g(t) = 1$, $f(t) = e^t - 1$. Note that $\left\{ {n \atop k} \right\}$ is the Stirling number of the second kind. It was further extended in [24] onto r-Bell polynomials ($g(t) = e^{rt}$, $f(t) = e^t - 1$) as well. Similar congruences hold for factorial polynomials ($g(t) = 1$, $f(t) = \ln(1+t)$; $S(n, k)$ are then the Stirling numbers of the first kind): $P_{n+p}(x) \equiv (x^p - x)S_n(x) \pmod{p}$ and derangement polynomials ($g(t) = e^{-t}/(1-t)$, $f(t) = t$): $D_{n+p} \equiv (x^p - 1)D_n(x) \pmod{p}$. Finally, let us remark that all these congruences can be expressed in the language of the coefficients $S(n, k)$, which might be understood as generalized Stirling numbers. For example, (1.2) is equivalent to

$$S(n + p, k) \equiv S(n, k - p) + S(n + 1, k) \pmod{p}, \quad 0 \leq k \leq n + p.$$

In the literature, there there are many results on congruences concerning the Bell numbers and Touchard polynomials [2, 13, 14, 15, 16, 26, 32, 35, 37], related sequences [41, 31, 24], and other Sheffer sequences [1, 4, 19, 36, 40].

The main goal of the paper is to examine whether the aforementioned congruences are driven by more universal laws. In order to make the investigation somehow systematic, we begin with a general congruence (see Lemma 2.1) for $n = 0$:

$$P_p(x) \equiv g_0 f_1 x^p + g_0 f_p x + g_p \pmod{p\mathbb{Z}[x]}. \tag{1.3}$$

Knowing that $P_0(x) = g_0$ and $P_1(x) = x g_0 f_1 + g_1$, we will express the right-hand side above by means of $P_0(x)$ and $P_1(x)$ and extend it onto all $n \in \mathbb{N}_0$. Obviously, there are many possibilities to consider, but we will focus, in the author's opinion, on the most natural and simple choices. First of all, we assume $g_0 \not\equiv 0 \pmod{p}$. Otherwise $P_p(x)$ is equivalent to a constant and the most straightforward extension leads to a sequence of constant polynomials of the trivial form $P_n(x) = g_n$.

Knowing the Touchard congruence (1.2), it is natural to look for it in (1.3). Indeed, if $f_p \equiv f_1$, $g_p \equiv g_1 \pmod{p}$, we get $P_p(x) \equiv x^p f_1 P_0(x) + P_1(x)$. Following this observation, we eventually reach the first main result of the article, Theorem 3.1, which states that the congruence

$$P_{n+p}(x) \equiv f_1 x^p P_n(x) + a P_{n+1}(x) \pmod{p\mathbb{Z}[x]} \tag{1.4}$$

holds if and only if $f_{n+p} \equiv a f_{n+1}$, $g_{n+p} \equiv a g_{n+1} \pmod{p}$ for every $n \in \mathbb{N}_0$. Note that an additional parameter $a \in \mathbb{Z}$ has been added to make the result more universal. Furthermore, we generalize (1.4) in Proposition 3.3 by providing congruences for $P_{n+kp^m}(x)$. See [14, 11] for the case of the Touchard polynomials.

Another approach to (1.3) is based on replacing any g_0 simply with $P_0(x)$ and g_p with $P_0(x)$ multiplied by some constant $a \in \mathbb{Z}$. This results in the congruence $P_p(x) \equiv (f_1x^p+f_px+a)P_0(x) \pmod{p\mathbb{Z}[x]}$, which appears to generalize conveniently into

$$P_{n+p}(x) \equiv (f_1x^p + f_px + a)P_n(x) \pmod{p\mathbb{Z}[x]}.$$

In Theorem 4.1, we precisely identify the class of sequences admitting this equivalence. Furthermore, this congruence takes a very appealing form of factorisation, if we additionally assume $g_0 \equiv 1 \pmod{p}$. Namely, we show in Corollary 4.3 that in this case the equivalence

$$P_{n+p}(x) \equiv P_p(x)P_n(x) \pmod{p\mathbb{Z}[x]}$$

holds if and only if $f_{n+1} \equiv 0$ and $g_{n+p} \equiv g_n \pmod{p}$ for $n \in \mathbb{N}_0$. Such a congruence has already appeared also in the context of non-Sheffer sequences. Namely, for the exponential generating function $\mathcal{H}_d(x)$ of the numbers of permutations being products of pairwise disjoint d-cycles, we define polynomials $W_{d,n}(x)$ by the relation $\frac{d^n}{dx^n}\mathcal{H}_d(x) = W_{d,n}(x)\mathcal{H}_d(x)$. Then, for any prime p and $n \in \mathbb{N}_0$ it holds that ([25], Theorem 6.7)

$$W_{p,n+p}(x) \equiv W_{p,p}W_{p,n} \pmod{p\mathbb{Z}[x]}.$$

Another interesting and intensively studied problem is the modular periodicity. This concerns the numbers P_n rather than polynomials $P_n(x)$. In [13] Marshall Hall showed that

$$N_p := 1 + p + \ldots + p^{p-1} = \frac{p^p - 1}{p - 1}$$

is a period of the sequence of Bell numbers $B_n = B_n(1)$ modulo p. This holds true for r-Bell numbers as well (see [24, 33]). Theorem (5.2) demonstrates that the sufficient condition for such a property is simply satisfying the Touchard congruence ((1.2) with $x = 1$). Note that this requires $f_1 \equiv a \equiv 1 \pmod{p}$ in (1.4). If $f_1 \not\equiv 1 \pmod{p}$, one can consider $P_n(x_0)$ instead of $P_n = P_n(1)$ for x_0 being the inverse of f_1 in $GF(p)$. In the case $a \not\equiv 1 \pmod{p}$, we refer the reader to Section 5 for some more details. It is also worth mentioning that even in the case of Bell numbers N_p is proven to be the minimal period only for $p < 126$ and for $p = 137, 149, 157, 163, 167, 173$ [20, 26, 39]. See [7, 21, 33] for further results in this direction.

The approach to the problem is strongly based on the exponential generating function (1.1). This tool seems to be slightly forgotten, while it still remains one of the most powerful. In the form of the characteristic function or the Fourier transform, it plays a crucial rule in probability theory. One of the reasons, in the context of the article, is that it allows one to deal with such a generality. For example, in the case of the Touchard congruence, a particular form of studied polynomials was exploited, which allowed one to conveniently employ the umbral calculus [4, 13, 24].

2 Preliminaries

2.1 Notation

Throughout the article, p stands for any prime number. By $\mathbb{N}_0$ we denote the set of non-negative integers. Furthermore, by $\mathbb{Z}[x]$ we understand the ring of polynomials with integer coefficients.

For any formal series of functions $\varphi(t,x)=\sum_{n=0}^{\infty}\varphi_n(x)\frac{t^n}{n!}$ we define

$$(\varphi(\cdot,x))_n := \varphi_n(x). \tag{2.1}$$

If φ does not depend on x, we skip it in the above notation. In the case when the series is convergent for some $x\in\mathbb{R}$ and $t\in\mathbb{R}-\{0\}$, $(\varphi(\cdot,x))_n$ is simply the n-th derivative with respect to t at zero.

Finally, for $n\in\mathbb{N}_0$ and $q>0$ we denote by $[n]_q$ the q-analog of n, i.e.

$$[n]_q=\frac{1-q^n}{1-q} \text{ for } q\neq 1, \qquad [n]_1=n. \tag{2.2}$$

2.2 Sheffer sequences

We have defined Sheffer sequences $(P_n(x))_{n\geq 0}$ in (1.1). Using the notation from equation (2.1), one can simply write

$$P_n(x)=\left(\mathbf{G}(\cdot,x)\right)_n.$$

They might be equivalently introduced by the recurrence $QP_n=nP_{n-1}$ for $n\geq 1$ and $QP_0=0$, where Q is a shift-equivariant linear operator acting on polynomials. Additionally, following the notation from [30], we may say that $P_n(x)$ is the Sheffer sequence for the pair $\left(1/g(\bar{f}(t)),\bar{f}(t),\right)$, where $\bar{f}(t)$ is the compositional inverse of $f(t)$. This nomenclature is related to the algebraic approach related to orthogonality properties of the polynomials.

The history of Sheffer polynomials dates back to the seminal paper [34]. The modern approach has been presented in [30]. We also refer the reader to [10] for an overview of the development of the theory, and to [8, 9, 17, 22, 29] for some recent advances.

For a Sheffer sequence $(P_n(x))_{n\geq 0}$ we define $(\widetilde{P}_n(x))_{n\geq 0}$ (the associated sequence for $\bar{f}(t)$) as the sequence whose exponential generating function is given by

$$\widetilde{\mathbf{G}}(t,x):=\sum_{n=1}^{\infty}\widetilde{P}_n(x)\frac{t^n}{n!}=e^{xf(t)},$$

which arised from (1.1) by taking $g(t)=1$. Then, the following binomial-like identity holds

$$\sum_{k=0}^{n}\binom{n}{k}P_k(x)\widetilde{P}_{n-k}(y)=P_n(x+y).$$

Furthermore, since

$$\frac{\partial}{\partial t}(g(t)e^{xf(t)}) = g'(t)e^{xf(t)} + xf'(t)g(t)e^{xf(t)}, \tag{2.3}$$

the Sheffer sequence satisfies the recurrence

$$P_{n+1}(x) = \sum_{k=0}^{n} \binom{n}{k} \left[xf_{k+1}P_{n-k}(x) + g_{k+1}\widetilde{P}_{n-k}(x) \right]. \tag{2.4}$$

The coefficients of $P_n(x) = \sum_{k=0}^{n} S(n,k)x^k$ are given by

$$S(n,k) = \frac{1}{k!}(gf^k)_n. \tag{2.5}$$

In particular, for $n \geq 1$ we have

$$\begin{aligned} S(n,0) &= g_n, \\ S(n,1) &= (gf)_n, \\ S(n,n) &= g_0 f_1^n. \end{aligned} \tag{2.6}$$

Here, the product of two formal power series is understood simply as the Cauchy product. The equality (2.6) follows from the assumption $f_0 = 0$. It also explains the assumption $f_1, g_0 \neq 0$, since the degree of any $P_n(x)$ is supposed to be n. Additionally, since $f_n, g_n \in \mathbb{Z}$, all the coefficients $S(n,k)$ are integers, which might be deduced e.g. from (2.4). Below, we present congruences for $S(n,k)$ with $n = p$, that are the initial point of our considerations.

Lemma 2.1 *For a prime p we have*

$$\begin{aligned} S(p,1) &\equiv g_0 f_p \pmod p, \\ S(p,p) &\equiv g_0 f_1 \pmod p, \\ S(p,k) &\equiv 0 \pmod p, \qquad 2 \leq k \leq p-1. \end{aligned}$$

Equivalently,

$$P_p(x) \equiv g_0 f_1 x^p + g_0 f_p x + g_p \pmod p. \tag{2.7}$$

Proof. First, by (2.5) and Lucas's congruence, we get

$$S(p,1) = (gf)_p = \sum_{i=0}^{p} \binom{p}{i} g_i f_{p-1} \equiv g_0 f_p + g_p f_0 = g_0 f_p \pmod p.$$

The congruence for $S(p,p)$ follows from (2.6) and Fermat's little theorem. Next, for $2 \leq k \leq p-1$ the general Leibniz formula and Lucas's congruence give us

$$\begin{aligned} S(p,k) = \frac{(gf^k)_p}{k!} = \frac{(f \cdot gf^{k-1})_p}{k!} &= \frac{1}{k!} \sum_{i=0}^{p} \binom{p}{i} f_i (gf^{k-1})_{p-i} \\ &\equiv \frac{1}{k!} \left(f_0 (gf^{k-1})_p + f_p g_0 f_0^{k-1} \right) = 0 \pmod p, \end{aligned}$$

where the last equality follows from the general assumption $f_0 = 0$. Finally, the equivalence (2.7) is a consequence of (2.5). □

An important subclass of the Sheffer polynomials are the Appell polynomials. Namely, we obtain them for $f(t) = t$. Note that, by the formula (2.5) and the general Leibniz rule, their coefficients take the form

$$S(n,k) = \binom{n}{k} g_{n-k}.$$

It is therefore sometimes more reasonable simply to consider the sequence (g_n).

2.3 Technical lemmas

In this section we gather two lemmas on divisibility properties of coefficients of formal power series. For convenience of proofs, they are described in the language of p-adic integers $\mathbb{Z}_p$.

Lemma 2.2 *Let u, v be formal power series with integer coefficients. Assume that $u_0 \not\equiv 0 \pmod p$ and fix $a \in \mathbb{Z}$. Then*

$$u_{n+p} \equiv a u_{n+1},\ w_{n+p} \equiv a w_{n+1} \pmod{p\mathbb{Z}_p} \quad \text{for all } n \geq 0$$
$$\Updownarrow$$
$$u_{n+p} \equiv a u_{n+1},\ (uw)_{n+p} \equiv a(uw)_{n+1} \pmod{p\mathbb{Z}_p} \quad \text{for all } n \geq 0.$$

Proof. ($\Downarrow$) By the general Leibniz rule applied twice we have for $n \geq 0$ that

$$(uv)_{n+p} = \sum_{i=0}^{n} \sum_{j=0}^{p} \binom{n}{i}\binom{p}{j} u_{i+j} w_{n+p-i-j}.$$

By virtue of Lucas's congruence we obtain

$$\begin{aligned}(uv)_n &\equiv \sum_{i=0}^{n} \binom{n}{i} (u_i w_{n+p-i} + u_{i+p} w_{n-i}) \equiv a \sum_{i=0}^{n} \binom{n}{i} (u_i w_{n+1-i} + u_{i+1} w_{n-i}) \\ &= a[(uw')_n + (u'w)_n] = a(uw)_{n+1} \pmod{p\mathbb{Z}_p}.\end{aligned}$$

($\Uparrow$) Due to the assumption $u_0 \not\equiv 0$ we can write

$$w = \frac{uw}{u} = \frac{uw}{u_0[1-(1-u/u_0)]} = \frac{uw}{u_0} \sum_{k=0}^{\infty} (1-u/u_0)^k. \tag{2.8}$$

From the previous implication (and by an induction argument) we know that for any $i, n \geq 0$ it holds that $(1-u/u_0)^k_{n+p} \equiv a(1-u/u_0)^k_{n+1} \pmod{p\mathbb{Z}_p}$. Thus, for $n \geq 0$ we have

$$\begin{aligned}\left(\sum_{k=0}^{\infty} (1-u/u_0)^k\right)_{n+p} &= \sum_{k=0}^{\infty} (1-u/u_0)^k_{n+p} \equiv \sum_{k=0}^{\infty} a(1-u/u_0)^k_{n+1} \\ &= \left(\sum_{k=0}^{\infty} a(1-u/u_0)^k\right)_{n+1} \pmod{p\mathbb{Z}_p},\end{aligned}$$

and applying the previous implication to (2.8) we complete the proof. □

Lemma 2.3 *Under the assumptions of the previous lemma we have*

$$u_n, w_n \equiv 0 \pmod{p\mathbb{Z}_p} \quad \text{for all } n \geq p$$
$$\Updownarrow$$
$$u_n, (uw)_n \equiv 0 \pmod{p\mathbb{Z}_p} \quad \text{for all } n \geq p.$$

Proof. ($\Downarrow$) We have

$$(uw)_n = \sum_{k=0}^{n} \binom{n}{k} u_k w_{n-k} \equiv \sum_{k=n-p+1}^{p-1} \frac{n!}{k!(n-k)!} u_k w_{n-k} \pmod{p\mathbb{Z}_p}.$$

Since $k, (n-k) \leq p-1$, the denominator in the quotient under the sum is not divisible by p, while the numerator is for $n \geq p$. Hence, every term is divisible by p, and therefore $(uw)_n \equiv 0 \pmod{p\mathbb{Z}_p}$ for $n \geq p$.

($\Uparrow$) The proof in this case is analogous to the corresponding part of the proof of Lemma 2.2. □

3 Touchard congruence

The Touchard congruence turns out to be not an exclusive property of the Touchard polynomials and Bell numbers or their weighted version. Below we present necessary and sufficient conditions for a Sheffer sequence to possess this property, even in a more general form.

Theorem 3.1 *Let p be a prime number and $a \in \mathbb{Z}$. The equivalence*

$$P_{n+p}(x) \equiv x^p f_1 P_n(x) + a P_{n+1}(x) \pmod{p\mathbb{Z}[x]}, \qquad n \geq 0, \tag{3.1}$$

holds if and only if

$$f_{n+p} \equiv a f_{n+1} \quad \text{and} \quad g_{n+p} \equiv a g_{n+1} \pmod{p}, \qquad n \geq 0.$$

Proof. ($\Rightarrow$) Assuming (3.1) holds, we get

$$g_{n+p} = S(n+p, 0) \equiv a S(n+1, 0) = a g_{n+1} \pmod{p},$$

and

$$(gf)_{n+p} = S(n+p, 1) \equiv a S(n+1, 1) = a (gf)_{n+1} \pmod{p}.$$

Next, by Lemma 2.2, we conclude $f_{n+p} \equiv a f_{n+1} \pmod{p}$, $n \geq 0$.

($\Leftarrow$) For $n = 0$ we use Lemma 2.1 and get

$$P_p(x) \equiv x^p g_0 f_1 + a x g_0 f_1 + a g_1 = x^p f_1 P_0(x) + a P_1(x) \pmod{p\mathbb{Z}[x]},$$

as required. Assume now that the congruence (3.1) holds for $n \leq N$ for some $N \geq 0$ and any sequence $(P_n(x))_{n \geq 0}$ satisfying the assumptions of the theorem. In

particular, the sequence $(\widetilde{P}_n(x))_{n\geq 0}$ is included. Furthermore, the relation (2.3) gives us

$$P_{N+1+p}(x) = \left[\left(g' + xgf'\right)\widetilde{\mathbf{G}}(\cdot,x)\right]_{N+p} = \left[g'\widetilde{\mathbf{G}}(\cdot,x) + xf'\mathbf{G}(\cdot,x)\right]_{N+p}. \tag{3.2}$$

Thus, using the general Leibniz rule twice we obtain

$$P_{N+1+p}(x) = \sum_{i=0}^{p}\sum_{j=0}^{N}\binom{p}{i}\binom{N}{j}\left[g_{i+j+1}\widetilde{P}_{N+p-i-j}(x) + xf_{i+j+1}P_{N+p-i-j}\right]. \tag{3.3}$$

Now we split the above sum into two parts. Using Lucas's congruence and the inductive assumption we deal with the first one as follows

$$\begin{aligned}
&\sum_{i=0}^{p}\sum_{j=0}^{N}\binom{p}{i}\binom{N}{j}g_{i+j+1}\widetilde{P}_{N+p-i-j}(x)\\
&\equiv \sum_{j=0}^{N}\binom{N}{j}\left[g_{j+1}\widetilde{P}_{N+p-j}(x) + g_{p+j+1}\widetilde{P}_{N-j}(x)\right]\\
&\equiv \sum_{j=0}^{N}\binom{N}{j}\left[g_{j+1}\left(x^p f_1\widetilde{P}_{N-j}(x) + a\widetilde{P}_{N-j+1}(x)\right) + ag_{j+2}\widetilde{P}_{N-j}(x)\right]\\
&= f_1x^p(g'\widetilde{\mathbf{G}}(\cdot,x))_N + a\left((g'\widetilde{\mathbf{G}}'(\cdot,x))_N + (g''\widetilde{\mathbf{G}}(\cdot,x))_N\right)\\
&= f_1x^p(g'\widetilde{\mathbf{G}}(\cdot,x))_N + a(g'\widetilde{\mathbf{G}}(\cdot,x))_{N+1} \pmod{p\mathbb{Z}[x]},
\end{aligned} \tag{3.4}$$

and, analogously, we get

$$\sum_{i=0}^{p}\sum_{j=0}^{N}\binom{p}{i}\binom{N}{j}f_{i+j+1}P_{N+p-i-j}(x) \equiv f_1x^p(f'\mathbf{G}(\cdot,x))_N + a(f'\mathbf{G}(\cdot,x))_{N+1} \pmod{p\mathbb{Z}[x]}.$$

Summing up, we arrive at

$$\begin{aligned}
P_{N+1+p}(x) &\equiv f_1x^p(g'\widetilde{\mathbf{G}}(\cdot,x) + xf'\mathbf{G}(\cdot,x))_N + a(g'\widetilde{\mathbf{G}}(\cdot,x) + xf'\mathbf{G}(\cdot,x))_{N+1} \pmod{p\mathbb{Z}[x]}\\
&= f_1x^pP_{N+1}(x) + aP_{N+2}(x),
\end{aligned}$$

where the last inequality is a consequence of (2.3). □

Note that for $\mathbb{Z} \ni f_1, a \equiv 1 \pmod p$ (3.1) becomes the classical Touchard congruence.

Let $((TP)_n(x))_{n\geq 0}$ be the binomial transform of $(P_n(x))_{n\geq 0}$, i.e.

$$(TP)_n(x) = \sum_{i=0}^{n}(-1)^k\binom{n}{k}P_k(x).$$

Corollary 3.2 *If the sequence $(P_n(x))_{n\geq 0}$ satisfies (3.1), then*

$$(TP)_{n+p}(x) \equiv -x^pf_1(TP)_n(x) + a(TP)_{n+1}(x) \pmod{p\mathbb{Z}[x]}.$$

Proof. The exponential generating function of $((TP)_n(x))_{n\geq 0}$ is

$$\sum_{n=0}^{\infty}(TP)_n\frac{t^n}{n!}=e^t g(t)e^{xf(-t)}.$$

We clearly have

$$f_{n+p}\equiv af_{n+1}\pmod p \quad\Leftrightarrow\quad (f(-(\cdot)))_{n+p}\equiv a(f(-(\cdot)))_{n+1}\pmod p,\qquad n\geq 0.$$

Furthermore, in view of the congruences

$$\begin{aligned}\left(e^{(\cdot)}\right)_{n+p}&=1=\left(e^{(\cdot)}\right)_{n+1},\\ (f(-(\cdot)))_1&\equiv -f_1,\end{aligned}$$

(mod p), the assertion follows from Theorem 3.1 and Lemma 2.2. □

We finish this section with some generalizations of Theorem 3.1 involving powers of p and their multiplicities. They play an important role in Section 5.

Proposition 3.3 *Let p be a prime number, $k\in\mathbb{N}_0$, $m\geq 1$ and $a\in\mathbb{Z}$. Then (3.1) implies*

$$P_{n+kp^m}(x)\equiv\sum_{i=0}^{k}\binom{k}{i}a^{mi}f_1^{k-i}(a^{m-1}x^p+a^{m-2}x^{p^2}+\ldots+x^{p^m})^{k-i}P_{n+i}(x)\pmod{p\mathbb{Z}[x]}.$$

Proof. We prove the proposition by mathematical induction with respect to m. The case $m=1$ is covered by (3.1) and another induction argument with respect to k with the following induction step:

$$\begin{aligned}P_{n+(k+1)p}(x)&=P_{n+p+kp}(x)\\ &\equiv\sum_{i=0}^{k}\binom{k}{i}a^i f_1^{k-i}(x^p)^{k-i}P_{n+i+p}(x)\\ &\equiv\sum_{i=0}^{k}\binom{k}{i}a^i f_1^{k-i}(x^p)^{k-i}\left[x^p f_1P_{n+i}(x)+aP_{n+i+1}\right]\pmod{p\mathbb{Z}[x]}\\ &=f_1^{k+1}(x^p)^{k+1}P_n(x)+\sum_{i=1}^{k}\left[\binom{k}{i}+\binom{k}{i-1}\right]a^i f_1^{k+1-i}(x^p)^{k+1-i}P_{n+i}(x)\\ &\quad+a^{k+1}P_{n+k+1}(x)\\ &=\sum_{i=0}^{k+1}\binom{k+1}{i}a^i f_1^{k+1-i}(x^p)^{k+1-i}P_{n+i}(x).\end{aligned}$$

Let us assume now that the assertion is satisfied for some $m\geq 1$ and all $k\in\mathbb{N}_0$. Lucas's congruence and Fermat's little theorem give us

$$P_{n+kp^{m+1}}=P_{n+(kp)p^m}$$

$$\equiv \sum_{l=0}^{kp} \binom{kp}{l} a^{ml} f_1^{kp-l} \left(a^{m-1}x^p + a^{m-2}x^{p^2} + \cdots + x^{p^m}\right)^{kp-l} P_{n+l}(x)$$
$$\equiv \sum_{i=0}^{k} \binom{k}{i} a^{imp} f_1^{kp-ip} \left(a^{m-1}x^p + a^{m-2}x^{p^2} + \cdots + x^{p^m}\right)^{kp-ip} P_{n+ip}(x)$$
$$\equiv \sum_{i=0}^{k} \binom{k}{i} a^{im} f_1^{k-i} \left(a^{m-1}x^{p^2} + a^{m-2}x^{p^3} + \cdots + x^{p^{m+1}}\right)^{k-i} \sum_{j=0}^{i} \binom{i}{j} a^j f_1^{i-j} (x^p)^{i-j} P_{n+j}(x) \pmod{p\mathbb{Z}[x]}.$$

Changing the order of summation we get

$$\sum_{j=0}^{k} \binom{k}{j} f_1^{k-j} P_{n+j}(x) a^{(m+1)j} \times \sum_{i=j}^{k} \binom{k-j}{i-j} \left(a^{m-1}x^{p^2} + a^{m-2}x^{p^3} + \ldots + x^{p^{m+1}}\right)^{(k-j)-(i-j)} (a^m x^p)^{i-j}$$
$$= \sum_{j=0}^{k} \binom{k}{j} f_1^{k-j} P_{n+j}(x) a^{(m+1)j} \left(a^m x^p + a^{m-1}x^{p^2} + a^{m-2}x^{p^3} + \ldots + x^{p^{m+1}}\right)^{k-j}.$$

This ends the proof. □

In particular, taking $k = 1$ or $m = 1$, we get

Corollary 3.4 *We have*

$$P_{n+p^m}(x) \equiv f_1 \left[\sum_{i=1}^{m} a^{m-i} x^{p^i}\right] P_n(x) + a^m P_{n+1}(x) \pmod{p\mathbb{Z}[x]}, \tag{3.5}$$
$$P_{n+kp}(x) \equiv \sum_{i=0}^{k} \binom{k}{i} a^i f_1^{k-i} x^{p(k-i)} P_{n+i}(x) \pmod{p\mathbb{Z}[x]},$$

or, equivalently,

$$S(n+p^m, l) \equiv f_1 \sum_{i=1}^{m} a^{m-i} S(n, l-p^i) + a^m S(n+1, l) \pmod{p},$$
$$S(n+kp, l) \equiv \sum_{i=0}^{k} \binom{k}{i} a^{k-i} f_1^i S(n+k-i, l-ip) \pmod{p}.$$

4 Multiplicative congruence

Due to the orthogonality property of the Stirling numbers of both kinds we can see a relation between Touchard and factorial polynomials, as their coefficients are given by the aforementioned numbers. The previous section was devoted to general rules standing behind divisibility properties of Touchard polynomials. In this section, we present congruences linked to the factorial ones. Namely, we will investigate when $P_{n+p}(x)$ is equivalent to $P_n(x)$ multiplied by a fixed polynomial. This kind of congruence has been studied for Appell polynomials in [3].

Theorem 4.1 *Let p be a prime number and $a \in \mathbb{Z}$. Then*

$$P_{n+p}(x) \equiv (f_1 x^p + f_p x + a) P_n(x) \pmod{p\mathbb{Z}[x]} \tag{4.1}$$

holds for any $n \in \mathbb{N}_0$ if and only if

$$f_{n+p+1} \equiv 0 \text{ and } g_{n+p} \equiv a g_n \pmod{p} \text{ for } n \geq 0. \tag{4.2}$$

Proof. ($\Rightarrow$) Due to the terms x^p and x on the right-hand side we have

$$g_{n+p} = S(n+p,0) \equiv aS(n,0) = ag_n \pmod{p}, \qquad n \geq 0.$$

This proves the congruence for the series g. Similarly, comparing coefficients of the term x, we obtain

$$(gf)_{n+p} = S(n+p,1) \equiv f_p S(n,0) + aS(n,1) = f_p g_n + a(gf)_n \pmod{p}.$$

Due to Lucas's congruence and (4.2) we may rewrite the left-hand side as follows

$$\begin{aligned}(gf)_{n+p} &= \sum_{i=0}^{p}\sum_{j=0}^{n}\binom{p}{i}\binom{n}{j} g_{n+p-i-j} f_{i+j} \\ &\equiv \sum_{j=0}^{n}\binom{n}{j}\left[g_{n+p-j} f_j + g_{n-j} f_{j+p}\right] \\ &\equiv a(gf)_n + \sum_{j=0}^{n}\binom{n}{j} g_{n-j} f_{j+p} \qquad \pmod{p\mathbb{Z}[x]}.\end{aligned}$$

Thus, we get

$$\sum_{j=1}^{n}\binom{n}{j} g_{n-j} f_{j+p} \equiv 0 \pmod{p}, \qquad n \geq 1.$$

Using this and mathematical induction with respect to n, we will show the desired congruence concerning the series f. Taking $n = 1$, we conclude $g_0 f_{p+1} \equiv 0 \pmod{p}$. Due to the assumption $g_0 \not\equiv 0 \pmod{p}$, we have $f_{p+1} \equiv 0 \pmod{p}$. Assume now that $f_{p+j} \equiv 0 \pmod{p}$ for $1 \leq j \leq m$ for some $m \geq 1$. Then

$$0 \equiv \sum_{j=1}^{m+1}\binom{n}{j} g_{m+1-j} f_{j+p} \equiv \sum_{j=1}^{m}\binom{n}{j} g_{m+1-j} \cdot 0 + g_0 f_{m+p+1} \equiv g_0 f_{m+p+1} \pmod{p},$$

which implies $f_{m+p+1} \equiv 0 \pmod p$, as required.

($\Leftarrow$) This part of the proof is similar to the corresponding part of the proof of Theorem 3.1. For $N = 0$ the assertion is true in view of Lemma 2.1. Assume that the congruence (4.1) holds for $n \le N$ for some $N \ge 0$ and any sequence $(P_n(x))_{n\ge 0}$ satisfying (4.2) for any $a \in \mathbb{Z}$. In particular, for such a sequence $\big(P_n(x)\big)_{n\in\mathbb{N}_0}$, the sequence $\big(\widetilde{P}_n(x)\big)_{n\in\mathbb{N}_0}$ satisfies (4.2) with $a = 0$. Then, similarly to (3.4), by virtue of Lucas's congruence, the inductive assumption and (4.2), we get

$$\begin{aligned}
&\sum_{i=0}^{p}\sum_{j=0}^{N}\binom{p}{i}\binom{N}{j} g_{i+j+1}\widetilde{P}_{N+p-i-j}(x)\\
&\equiv \sum_{j=0}^{N}\binom{N}{j}\Big[g_{j+1}\widetilde{P}_{N+p-j}(x) + g_{p+j+1}\widetilde{P}_{N-j}(x)\Big]\\
&\equiv \sum_{j=0}^{N}\binom{N}{j} g_{j+1}\big(f_1x^p + f_px + a\big)\widetilde{P}_{N-j}(x)\\
&= \big(f_1x^p + f_px + a\big)(g'\widetilde{\mathbf{G}}(\cdot,x))_N \pmod{p\mathbb{Z}[x]},
\end{aligned}$$

as well as

$$\sum_{i=0}^{p}\sum_{j=0}^{N}\binom{p}{i}\binom{N}{j} f_{i+j+1}P_{N+p-i-j}(x) \equiv \big(f_1x^p + f_px + a\big)(f'\mathbf{G}(\cdot,x))_N \pmod{p\mathbb{Z}[x]}.$$

Applying these to (3.3) and using (3.2) we get

$$\begin{aligned}
P_{N+p+1}(x) &\equiv (f_1x^p + f_px + a)\Big[g'\widetilde{\mathbf{G}}(\cdot,x) + xf'\mathbf{G}(\cdot,x)\Big]_N\\
&= (f_1x^p + f_px + a)P_{N+1}(x) \pmod{p\mathbb{Z}[x]}.
\end{aligned}$$

The proof is complete. □

Remark 4.2 Verifying whether g (for $a = 0$) or f (if $f_p \equiv 0 \pmod p$) satisfy the assumptions of the theorem, one can find Lemma 2.3 helpful. In particular, it follows that for a formal power series h with integer coefficients and $h_0 = 1$ it holds $h_n, (\frac{1}{h})_n \equiv 0 \pmod p$ for $n \ge p$ if and only if $h_n, 1_n \equiv 0 \pmod p$ for $n \ge p$. Thus, for $f = \frac{1}{h} - 1$ the congruence $f_n \equiv 0 \pmod p$ is valid for $n \ge p$ if and only if $h_n \equiv 0 \pmod p$ for $n \ge p$.

The congruence (4.1) takes an especially elegant form, if $g_0 \equiv 1$ and $g_p \equiv a \pmod p$. In that case, by (2.7), we have $(f_1x^p + f_px + a) \equiv P_p(x) \pmod{p\mathbb{Z}[x]}$. In the corollary below, we do not require $g_p \equiv a \pmod p$, as it follows from other assumptions.

Corollary 4.3 *Let p be a prime number and $g_0 \equiv 1 \pmod p$. Then*

$$P_{n+p}(x) \equiv P_p(x)P_n(x) \pmod{p\mathbb{Z}[x]} \tag{4.3}$$

holds for any $n \in \mathbb{N}_0$ if and only if

$$f_{n+p+1} \equiv 0 \text{ and } g_{n+p} \equiv g_pg_n \pmod p \text{ for } n \ge 0.$$

5 Modular periodicity

In this section, we investigate modular periods of the Sheffer sequences, which are the smallest numbers $N \in \mathbb{N} = \{1, 2, 3, \ldots\}$ such that $P_{n+N} \equiv P_n \pmod p$. In the case of sequences considered in Theorem 4.1, the answer is quite simple. If $f_1 + f_p + a \equiv 1 \pmod p$, then we have $N = p$. If $f_1 + f_p + a \equiv 0 \pmod p$, then $P_n \equiv 0 \pmod p$ for $n \geq p$. In the remaining case, when $f_1 + f_p + a$ is congruent neither to 0 nor to 1, let k be the multiplicative order of $f_1 + f_p + a$. Then N equals pk or divides k. Note that the situation is similar in the setting of Theorem 3.1, if $a \equiv 0$ or $f_1 \equiv 0 \pmod p$.

The case described in Theorem 3.1 with $a \not\equiv 0 \pmod p$ is more complex. Using the notation (2.2) of q-analogs, the equivalence (3.5) with $x = 1$ takes the form

$$P_{n+p^m} \equiv f_1[m]_a P_n + a^m P_{n+1} \pmod p, \qquad n, m \in \mathbb{N}_0. \tag{5.1}$$

This somehow explains how q-analogs appear in this theory. The q-Stirling numbers of the first kind $\begin{bmatrix} n \\ k \end{bmatrix}_q$ are defined by the formula

$$x(x + [1]_q)(x + [2]_q) \cdot \ldots \cdot (x + [n-1]_q) = \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix}_q x^k,$$

with $\begin{bmatrix} 0 \\ 0 \end{bmatrix}_q = 1$. The recursive relation is analogous as in the classical case ([12], formula (3.20)):

$$\begin{bmatrix} n+1 \\ k \end{bmatrix}_q = [n]_q \begin{bmatrix} n \\ k \end{bmatrix}_q + \begin{bmatrix} n \\ k-1 \end{bmatrix}_q, \quad 0 \leq k \leq n. \tag{5.2}$$

The next proposition is the key one in proving Theorem 5.2. It also shows the obstacles that occur when dealing with $a \not\equiv 1 \pmod p$.

Proposition 5.1 *Let $a \in \mathbb{N}_0$ be such that $a \not\equiv 0 \pmod p$. If $P_{n+p} \equiv f_1 P_n + a P_{n+1}$ for any $n, m \in \mathbb{N}_0$, then*

$$P_{n+p^1+\ldots+p^m} \equiv a^{\binom{m}{2}} \sum_{i=0}^{m} \begin{bmatrix} m+1 \\ i+1 \end{bmatrix}_{1/a} a^i f_1^{m-i} P_{n+i} \pmod p, \qquad n, m \in \mathbb{N}_0. \tag{5.3}$$

For $m = 0$ the left-hand side is interpreted as P_n.

Proof. For $m = 0$ the assertion is trivial. Assume (5.3) holds for some $m \in \mathbb{N}_0$. Then, by the congruence (5.1) and mathematical induction we get

$$\begin{aligned} P_{n+p^1+\ldots+p^{m+1}} &\equiv a^{\binom{m}{2}} \sum_{i=0}^{m} \begin{bmatrix} m+1 \\ i+1 \end{bmatrix}_{1/a} a^i f_1^{m-i} P_{n+i+p^{m+1}} \\ &\equiv a^{\binom{m}{2}} \sum_{i=0}^{m} \begin{bmatrix} m+1 \\ i+1 \end{bmatrix}_{1/a} a^i f_1^{m-i} \big(f_1 [m+1]_a P_{n+i} + a^{m+1} P_{n+i+1} \big) \pmod p \end{aligned}$$

$$= a^{\binom{m}{2}} a^m \sum_{i=0}^{m} \begin{bmatrix} m+1 \\ i+1 \end{bmatrix}_{1/a} a^i f_1^{m-i} \left(f_1 \frac{[m+1]_a}{a^m} P_{n+i} + a P_{n+i+1} \right).$$

Next, due to the equalities $[m+1]_a/a^m = [m+1]_{1/a}$ and (5.2) we get

$$\begin{aligned} P_{n+p^1+\ldots+p^{m+1}} &= a^{\binom{m+1}{2}} \sum_{i=0}^{m} \begin{bmatrix} m+1 \\ i+1 \end{bmatrix}_{1/a} a^i f_1^{m-i} \big(f_1 [m+1]_{1/a} P_{n+i} + a P_{n+i+1} \big) \\ &\equiv a^{\binom{m+1}{2}} \sum_{i=0}^{m+1} a^i f_1^{m+1-i} P_{n+i} \left([m+1]_{1/a} \begin{bmatrix} m+1 \\ i+1 \end{bmatrix}_{1/a} + \begin{bmatrix} m+1 \\ i \end{bmatrix}_{1/a} \right) \\ &\equiv a^{\binom{m+1}{2}} \sum_{i=0}^{m+1} a^i f_1^{m+1-i} P_{n+i} \begin{bmatrix} m+2 \\ i+1 \end{bmatrix}_{1/a}, \qquad \pmod p, \end{aligned}$$

where we also used $\begin{bmatrix} n \\ 0 \end{bmatrix}_{1/a} = 0$ for $n \geq 1$. □

As mentioned in the Introduction, the number

$$N_p := [p]_p = \frac{p^p - 1}{p-1}$$

is a period of the Bell numbers modulo p. Below, we show that this is a more general feature.

Theorem 5.2 *Assume $f_1 \not\equiv 0 \pmod p$. If $P_{n+p} \equiv f_1 P_n + P_{n+1} \pmod p$ for any $n \in \mathbb{N}_0$, then we we have*

$$P_{n+N_p} \equiv f_1 P_n \pmod p, \qquad n \geq 0.$$

Proof. Applying Proposition 5.1 with $m = p-1$ and $a = 1$, by Fermat's little theorem, Wilson's theorem and Lagrange's congruence ($\begin{bmatrix} p \\ i \end{bmatrix} \equiv 0 \pmod p$ for $2 \leq i \leq p-1$) we obtain

$$\begin{aligned} P_{n+N_p} &\equiv \sum_{i=0}^{p-1} \begin{bmatrix} p \\ i+1 \end{bmatrix} f_1^{p-1-i} P_{n+1+i} \\ &\equiv \begin{bmatrix} p \\ 1 \end{bmatrix} f_1^{p-1} P_{n+1} + \begin{bmatrix} p \\ p \end{bmatrix} P_{n+p} = (p-1)! f_1^{p-1} P_{n+1} + P_{n+p} \\ &\equiv -P_{n+1} + (f_1 P_n + P_{n+1}) = f_1 P_n \pmod p, \end{aligned}$$

as required. □

Unfortunately, the argument from the above proof cannot be adapted for $a \not\equiv 1$. The reason is that the q-analogs of the Stirling numbers of the first kind do not possess such convenient divisibility properties as their classical counterparts; see e.g. [31] for some examples for q being a natural number. In our case $q = 1/a$ is not natural, but we can for example verify that

$$\mathbb{N}_0 \ni a^{p-2} \begin{bmatrix} p \\ p-1 \end{bmatrix}_{1/a} = a^{p-2} \sum_{i=1}^{p-1} \frac{(1/a)^i - 1}{(1/a) - 1}$$

$$\begin{aligned} &= \frac{1-pa^{p-1}+(p-1)a^p}{(1-a)^2} \\ &\equiv (1-a)^{p-2} \pmod p, \end{aligned}$$

which is congruent to 0 only if $a \equiv 1 \pmod p$.

Nevertheless, this is not only a disadvantage of the proof. Let us present a precise example and consider $g(t) = 1$ and $f(t) = \sum_{k=0}^{\infty} \frac{a^k t^{k(p-1)+1}}{(k(p-1)+1)!}$. Then we have $P_k = f_1^k = 1$ for $0 \le k \le p-1$ and $P_p = f_1^p + f_p = 1 + a$. Next, by Proposition 5.1, we have

$$\begin{aligned} P_{N_p} &\equiv a^{\binom{p-1}{2}} \sum_{i=0}^{p-1} \begin{bmatrix} p \\ i+1 \end{bmatrix}_{1/a} a^i P_{i+1} \\ &= a^{\binom{p-1}{2}} \left(\sum_{i=0}^{p-1} \begin{bmatrix} p \\ i+1 \end{bmatrix}_{1/a} a^i + \begin{bmatrix} p \\ p \end{bmatrix}_{1/a} a^p \right) \\ &= a^{\binom{p-1}{2}} \left(a(a+[1]_{1/a})(a+[2]_{1/a}) \cdot \ldots \cdot (a+[p-1]_{1/a}) + a^p \right) \\ &= a[1]_a[2]_a \cdot \ldots \cdot [p]_a + a^{\binom{p-1}{2}+1} \pmod p. \end{aligned}$$

Fermat's little theorem implies $[p-1]_a \equiv 0 \pmod p$, thus $P_{N_p} \equiv a^{\binom{p-1}{2}+1} \pmod p$, which may not be congruent to $P_0 = 1$. We leave it as an open question what is the form of the period of P_n modulo p (if exists) for $a \not\equiv 0, 1 \pmod p$.

6 Examples

The first example is in fact one of the motivations of conducting the research described in this article. Now we will present how the classical Touchard congruence (1.2) follows from general theory developed before.

(1) **The Touchard (Bell) polynomials** $T_n(x)$**:** $g(t) = 1, f(t) = e^t - 1$.

Clearly, for $n \ge 1$ we have $f_n = 1$ and by Theorem 3.1 with $a = 1$ the Touchard congruence holds.

One of the strengths of the equivalence in Theorem 3.1 is that it shows that Sheffer polynomials satisfying the Touchard congruence for any prime p are relatively rare. It is not easy to produce such a non-trivial sequence. In the next example we narrow our attention to odd primes.

(2) **The central Bell polynomials** $B_n^c(x)$**:** $g(t) = 1, f(t) = 2\sinh(t/2)$.

The central Bell polynomials (see e.g. [6, 18]) are related to the Touchard (Bell) polynomials by the fact that the function $f(t) = f_T(t/2) - f_T(-t/2)$, where f_T is associated with the Touchard polynomials. Here, it holds that $f_n = 2^{1-n}\mathbf{1}_{\{2\nmid n\}}$ and therefore the polynomials $2^n B_n^c(x)$ satisfy the Touchard congruence with $a = 1$. It might be also reasonable to consider the polynomials $2^n B_n^c(x/2)$, since

then $f(t) = \sinh(t)$, $f_n = \mathbf{1}_{\{2\nmid n\}}$ and consequently the Touchard congruence is valid for odd primes p.

The next sequence satisfies the Touchard congruence for one chosen prime only.

(3) $g(t) = 1$, $f(t) = \sum_{n=1}^{\infty} \frac{t^{nk}}{(nk)!}$ for a fixed $k \in \{1, 2, 3, \ldots\}$.

In this case $g_n = \mathbf{1}_{\{n=0\}}$ and $f_n = \mathbf{1}_{\{k|n\}}$. Clearly, the assumptions of Theorem 3.1 are satisfied for $p \equiv 1 \pmod{k}$ only. Therefore $P_{n+p}(x) \equiv x^p P_n(x) + P_{n+1}(x) \pmod{p\mathbb{Z}[x]}$ for all $n \geq 0$ if and only if $p \equiv 1 \pmod{k}$.

In the following series of examples, some well-known polynomials are considered that satisfy the multiplicative congruence (4.3).

(4) **The factorial polynomials (rising factorials)** $x^{(n)} = x(x+1)\cdot\ldots\cdot(x+n-1)$**:** $g(t) = 1$, $f(t) = \ln(1+t)$.

The coefficients of these fundamental polynomials are the (unsigned) Stirling numbers of the first kind. Their divisibility properties are therefore well known and Corollary 4.3 simply recovers some of them. Nevertheless, the author has not found them presented in the form from the corollary.

(5) **The central factorial polynomials** $x^{[n]} = x(x - \frac{n}{2} + 1)^{(n-1)}$**:** $g(t) = 1$, $f(t) = 2\sinh^{-1}(t/2) = \sum_{k=0}^{\infty} \binom{2k}{k} \frac{(-1)^k}{2^{4k}} \frac{t^{2k+1}}{2k+1}$.

They are clearly related to the factorial polynomials, however, in a different manner than the central Bell polynomials are related to the Touchard polynomials, associated by their functions f.

Due to the non-integer values of the coefficients of the polynomials $x^{[n]}$, let us consider $2^n x^{[n]}$ and $p \geq 3$ (for $p = 2$ and $n \geq 1$ all the coefficients are even and consequently $2^n x^{[n]} \equiv 0 \pmod{p\mathbb{Z}[x]}$, $n \geq 1$). Unfortunately, the coefficients of f corresponding to $2^n x^{[n]}$ are still non-integers, hence we will pass through the polynomials $4^n x^{[n]}$. In that case we have $\tilde{g}_n = 0, n \geq 1$, and $\tilde{f}_n = 4(-1)^{(n-1)/2}(n-1)!\binom{n-1}{(n-1)/2}\mathbf{1}_{\{2\nmid n\}}$. Since $p|(n-1)!\mathbf{1}_{\{2\nmid n\}}$ for $n \geq p+1$, $\tilde{f}_1 = 4$ and, by Wilson's theorem, we have

$$\tilde{f}_p = 4(-1)^{(p-1)/2}\frac{[(p-1)!]^2}{[(\frac{p-1}{2})!]^2} \equiv 4(-1)^{(p-1)/2}\frac{[-1]^2}{(-1)^{(p+1)/2}} = -4 \pmod{p},$$

Theorem 4.1 with $a = 0$ implies the congruence

$$4^{n+p}x^{[n+p]} \equiv 4^p x^{[p]} 4^n x^{[n]} \equiv 4^{n+p}(x^p - x)x^{[n]} \pmod{p\mathbb{Z}[x]}, \qquad n \in \mathbb{N}_0.$$

Since $p \geq 3$ and $2^n x^{[n]} \in \mathbb{Z}[x]$, we can simply divide by 2^{n+p} and get

$$2^{n+p}x^{[n+p]} \equiv 2^{n+p} x^{[p]} x^{[n]} \equiv 2^{n+p}(x^p - x)x^{[n]} \pmod{p\mathbb{Z}[x]}, \qquad n \in \mathbb{N}_0.$$

(6) **The generalized Laguerre polynomials multiplied by factorials** $n!L_n^{(r)}(x)$: $g(t) = 1/(1-t)^{r-1}, f(t) = -t/(1-t)$, $r \in \mathbb{Z}$.

Similarly as in the previous example, the coefficients of the polynomials $L_n^{(r)}(x)$ are not integers and it is more convenient to consider the product of them and factorials $n!L_n(x)$. In particular, the coefficients of $n!L_n^{2r-1}(x)$ are the r-Lah numbers [27]. We clearly have $p|f_n = -n!$, $n \geq p$. Furthermore, since the coefficients of the power series g are integer, we have $p|(n+p)!|g_{n+p}$ for $n \geq 0$. Consequently, Theorem 4.1 with $a = 0$ gives us

$$L_{n+p}^{(r)}(x) \equiv L_p^{(r)}(x)L_n^{(r)}(x) \equiv x^p L_n^{(r)}(x) \pmod{p\mathbb{Z}[x]}, \quad n \in \mathbb{N}_0.$$

(7) **The derangement polynomials** $D_n(x)$**:** $g(t) = \frac{e^t}{1-t}, f(t) = t$. Here, $g_n = \sum_{k=0}^{n} \frac{n!}{k!}$. By Lucas's congruence we have

$$\begin{aligned} g_{n+p} - g_n &= \sum_{k=0}^{n+p} \frac{(n+p)!}{k!} - \sum_{k=0}^{n} \frac{n!}{k!} \equiv \sum_{k=0}^{n+p} \frac{(n+p)!}{k!} - \sum_{k=0}^{n} \frac{(n+p)!}{(k+p)!} \\ &= \sum_{k=0}^{p-1} \frac{(n+p)!}{k!} \pmod{p}. \end{aligned}$$

In the last sum, every term is divisible by p, hence $g_{n+p} \equiv g_n \equiv g_p g_n \pmod{p}$ for $n \geq 0$. Thus, Theorem 4.1 with $a = 1$ gives us

$$D_{n+p}(x) \equiv D_p(x)D_n(x) \equiv (x^p+1)D_n(x) \pmod{p\mathbb{Z}[x]}, \quad n \in \mathbb{N}_0.$$

(8) **The Hermite polynomials** $H_n(x)$**:** $g(t) = e^{-t^2/2}, f(t) = t$.

In this case it holds that $g_n = (-1)^{n/2}(n-1)(n-3)\cdot\ldots\cdot 1\cdot \mathbf{1}_{\{2|n\}}$ and $f_n = \mathbf{1}_{\{n=1\}}$. Thus, the Hermite polynomials satisfy the assumptions of Corollary 4.3 for prime $p \geq 3$. Since $f_p \equiv g_p \equiv 0 \pmod{p}$, Theorem 4.1 we have

$$H_{n+p}(x) \equiv H_p(x)H_n(x) \equiv x^p H_n(x) \pmod{p\mathbb{Z}[x]}, \quad n \in \mathbb{N}_0.$$

This could be deduced directly from the explicit formula of the polynomials as well

$$H_n(x) = n! \sum_{k=0}^{\lfloor n/2 \rfloor} \frac{(-1)^k}{2^k k!(n-2k)!} x^{n-2k}.$$

(9) **The Mott polynomials** $s_n(x)$**:** $g(t) = 1, f(t) = \left(\sqrt{1-t^2} - 1\right)/t$.

Here, we have $g_n = \mathbf{1}_{\{n=0\}}$ and $f_n = -\frac{n!C_{(n-1)/2}}{2^n}\mathbf{1}_{\{2\nmid n\}}$, where C_n are the Catalan numbers. The coefficients in the Mott polynomials are rational numbers with powers of 2 in denominators, so we will consider the polynomials $2^n s_n(x)$, similarly as in the case of the central factorial numbers. The corresponding coefficients f_n take then the form $\tilde{f}_n = 2^n f_n = -n!C_{(n-1)/2}\mathbf{1}_{\{2\nmid n\}}$. Since Catalan

numbers are integer numbers, $f'_n \equiv 0 \pmod p$ for $n \geq p$. Hence, by Theorem 4.1 with $a = 1$, we have

$$2^{n+p}s_{n+p}(x) \equiv 2^{n+p}s_p(x)s_n(x) \equiv 2^{n+p}x^p s_n(x) \pmod{p\mathbb{Z}[x]}, \quad n \in \mathbb{N}_0.$$

When considering congruences in the ring of polynomials with p-adic coefficients $\mathbb{Z}_p[x]$, one can clearly get rid of 2^{n+p} above, if $p \geq 3$.

(10) **The Mittag-Leffler polynomials** $M_n(x)$**:** $g(t) = 1, f(t) = 2\tanh^{-1} t = \ln\left(\frac{t+1}{t-1}\right)$.

Since $f_n = 2 \cdot (n-1)!\mathbf{1}_{\{2\nmid n\}}$, we have $f_n, g_n \equiv 0 \pmod p$ for $n \geq p \geq 3$ and, similarly as in the previous two examples, Theorem 4.1 for $a = 0$ gives us

$$M_{n+p}(x) \equiv M_p(x)M_n(x) \equiv x^p M_n(x) \pmod{p\mathbb{Z}[x]}, \quad n \in \mathbb{N}_0.$$

It is quite common in literature to consider so called r-polynomials by taking $g(t) = [f(t)]^r$, $r \in \mathbb{N}_0$. We will denote them by $P_{n,r}(x)$. This is how the r-Bell polynomials $B_{n,r}(x)$ [23], the "shifted" factorial polynomials $(x+r)^{(n)}$, and the polynomials $n!L_n^{(2r-1)}(x)$ arise. Equivalently, we deal with the r-Stirling numbers of both kinds [5] and the r-Lah numers. A similar procedure may be also applied to approach the r-derangement numbers [40].

(11) r**-polynomials** $P_{n,r}(x)$**:** $g(t) = [f'(t)]^r$.

By Theorem 3.1 and Lemma 2.2 we deduce that for fixed $a, r \in \mathbb{N}_0$ and prime p the congruence

$$P^{(r)}_{n+p}(x) \equiv x^p f_1 P^{(r)}_n(x) + aP^{(r)}_{n+1}(x) \pmod{p\mathbb{Z}[x]}, \quad n \in \mathbb{N}_0,$$

holds if and only if $f_{n+p} \equiv af_{n+1} \pmod p$ for $n \geq 0$. On the other hand, by Theorem 4.1 and Lemma 2.3 the congruence

$$P^{(r)}_{n+p}(x) \equiv P^{(r)}_p(x)P^{(r)}_n(x) \equiv (x^p + f_p x)P^{(r)}_n(x) \pmod{p\mathbb{Z}[x]}, \quad n \in \mathbb{N}_0,$$

holds if and only if $f_{n+p+1} \equiv 0 \pmod p$ for $n \geq 0$.

Acknowledgements

The author would like to thank the referees for their careful reading of the article and for providing many valuable comments and remarks that significantly improved the presentation of the paper.

References

[1] A. Adelberg, Universal higher order Bernoulli numbers and Kummer and related congruences, *J. Number Theory* **84** (2000), 119–135.

[2] H. W. Becker and J. Riordan, The arithmetic of Bell and Stirling numbers, *Amer. J. Math.* **70** (1948), 385–394.

[3] A. Benyattou, Congruences via umbral calculus, *Notes Number Theory Discrete Math.* **28** (2022), 719–729.

[4] A. Benyattou and M. Mihoubi, Curious congruences related to the Bell polynomials, *Quaest. Math.* **41** (2018), 437–448.

[5] A. Z. Broder, The r-Stirling numbers, *Discrete Math.* **49** (1984), 241–259.

[6] P. L. Butzer, M. Schmidt, E. L. Stark and L. Vogt, Central factorial numbers; their main properties and some applications, *Numer. Funct. Anal. Optim.* **10** (1989), 419–488.

[7] M. Car, L. H. Gallardo, O. Rahavandrainy and L. N. Vaserstein, About the period of Bell numbers modulo a prime, *Bull. Korean Math. Soc.* **45** (2008), 143–155.

[8] S. A. Carrillo and M. Hurtado, Appell and Sheffer sequences: on their characterizations through functionals and examples, *C. R. Math. Acad. Sci. Paris* **359** (2021), 205–217.

[9] G.-S. Cheon, T. Forgács, H. Kim and K. Tran, On combinatorial properties and the zero distribution of certain Sheffer sequences, *J. Math. Anal. Appl.i* **514** (2022), Paper No. 126273, 57.

[10] F. A. Costabile, M. I. Gualtieri and A. Napoli, Towards the centenary of sheffer polynomial sequences: Old and recent results, *Mathematics* **10** (2022).

[11] A. Gertsch and A. M. Robert, Some congruences concerning the Bell numbers, *Bull. Belg. Math. Soc. Simon Stevin* **3** (1996), 467–475.

[12] H. W. Gould, The q-Stirling numbers of first and second kinds, *Duke Math. J.* **28** (1961), 281–289.

[13] M. Hall, Arithmetic properties of a partition function, *Bull. Amer. Math. Soc.* **40** (1934).

[14] F. T. Howard, Congruences for the Stirling numbers and associated Stirling numbers, *Acta Arith.* **55** (1990), 29–41.

[15] A. Junod, Congruences pour les polynômes et nombres de Bell, *Bull. Belg. Math. Soc. Simon Stevin* **9** (2002), 503–509.

[16] N. Kahale, New modular properties of Bell numbers, *J. Combin. Theory Ser. A* **58** (1991), 147–152.

[17] S. Khan and M. Haneef, A note on the post quantum-sheffer polynomial sequences, *Forum Mathematicum* (2024).

[18] T. Kim and D. S. Kim, A note on central Bell numbers and polynomials, *Russ. J. Math. Phys.* **27** (2020), 76–81.

[19] E. Lehmer, On congruences involving Bernoulli numbers and the quotients of Fermat and Wilson, *Ann. Math.* (2) **39** (1938), 350–360.

[20] J. Levine and R. E. Dalton, Minimum periods, modulo p, of first-order Bell exponential integers, *Math. Comp.* **16** (1962), 416–423.

[21] W. F. Lunnon, P. A. B. Pleasants and N. M. Stephens, Arithmetic properties of Bell numbers to a composite modulus I, *Acta Arith.* **35** (1979), 1–16.

[22] A. Luzón, M. A. Morón and J. L. Ramírez, On Ward's differential calculus, Riordan matrices and Sheffer polynomials, *Linear Algebra Appl.* **610** (2021), 440–473.

[23] I. Mező, The r-Bell numbers, *J. Integer Sequ.* **14** (2011), Art. 11.1.1, 14.

[24] I. Mező and J. L. Ramírez, Divisibility properties of the r-Bell numbers and polynomials, *J. Number Theory* **177** (2017), 136–152.

[25] P. Miska and M. Ulas, On some properties of the number of permutations being products of pairwise disjoint d-cycles, *Monatsh. Math.* **192** (2020), 125–183.

[26] P. L. Montgomery, S. Nahm and S. S. Wagstaff, Jr., The period of the Bell numbers modulo a prime, *Math. Comp.* **79** (2010), 1793–1800.

[27] G. Nyul and G. Rácz, The r-Lah numbers, *Discrete Math.* **338** (2015), 1660–1666.

[28] C. Radoux, Une congruence pour les polynômes $P_n(x)$ de fonction génératrice $e^{x(e^z-1)}$, *C. R. Acad. Sci. Paris Sér. A-B* **284** (1977), A637–A639.

[29] M. Riyasat, A Riordan array approach to Apostol type—Sheffer sequences, *Filomat* **33** (2019), 6025–6038.

[30] S. Roman, "The umbral calculus", vol.xi 111 of Pure and Applied Mathematics, Academic Press, Inc. (Harcourt Brace Jovanovich, Publishers), New York, 1984.

[31] B. E. Sagan, Congruence properties of q-analogs, *Adv. Math.* **95** (1992), 127–143.

[32] G. Serafin, Identities behind some congruences for r-Bell and derangement polynomials, *Res. Number Theory* **6** (2020), Paper No. 39, 8.

[33] G. Serafin, Backward Touchard congruence, *Bull. Belg. Math. Soc. Simon Stevin* **28** (2022), 603–614.

[34] I. M. Sheffer, Some properties of polynomial sets of type zero, *Duke Math. J.* **5** (1939), 590–622.

[35] Y. Sun, X. Wu and J. Zhuang, Congruences on the Bell polynomials and the derangement polynomials, *J. Number Theory* **133** (2013), 1564–1571.

[36] Z.-H. Sun, Congruences for Bernoulli numbers and Bernoulli polynomials, *Discrete Math.* **163** (1997), 153–163.

[37] Z.-W. Sun and D. Zagier, On a curious property of Bell numbers, *Bull. Aust. Math. Soc.* **84** (2011), 153–158.

[38] J. Touchard, Propriétés arithmétiques de certains nombres récurrents, *Ann. Sot. Sci. Bruxelles Ser. A* **53** (1933), 21–31.

[39] S. S. Wagstaff, Jr., Aurifeuillian factorizations and the period of the Bell numbers modulo a prime, *Math. Comp.* **65** (1996), 383–391.

[40] C. Wang, P. Miska and I. Mező, The r-derangement numbers, *Discrete Math.* **340** (2017), 1681–1692.

[41] P. T. Young, Congruences for degenerate number sequences, *Discrete Math.* **270** (2003), 279–289.

(Received 21 Sep 2023; revised 1 Mar 2024, 16 Mar 2024)