ON HENSEL'S ROOTS AND A FACTORIZATION FORMULA IN $\mathbb{Z}[[X]]$

Daniel Birmajer
Department of Mathematics, Nazareth College, Rochester, New York
abirmaj6@naz.edu

Juan B. Gil
Penn State Altoona, Altoona, Pennsylvania
jgil@psu.edu

Michael D. Weiner
Penn State Altoona, Altoona, Pennsylvania
mdw8@psu.edu

Received: 8/27/13, Revised: 3/27/14, Accepted: 6/25/14, Published: 9/17/14

Abstract

Given an odd prime p, we provide formulas for the Hensel lifts of polynomial roots modulo p, and give an explicit factorization over the ring of formal power series with integer coefficients for certain reducible polynomials whose constant term is of the form p^w with $w > 1$. All of our formulas are given in terms of partial Bell polynomials and rely on the inversion formula of Lagrange.

1. Introduction

The divisibility theory of commutative rings is a fundamental and persisting topic in mathematics that entails two main aspects: determining irreducibility and finding a factorization of the reducible elements in the ring. Prominent examples are the ring of integers $\mathbb{Z}$ and the ring of polynomials $\mathbb{Z}[x]$. It is then natural to investigate the arithmetic properties of $\mathbb{Z}[[x]]$, the ring of formal power series with integer coefficients. While polynomials in $\mathbb{Z}[x]$ can be seen as power series over the integers, the factorization properties over $\mathbb{Z}[x]$ and over $\mathbb{Z}[[x]]$ are in general unrelated; cf. [4]. In [5], the authors studied this factorization problem exhaustively. In particular, for a class of polynomials parametrized by a prime p, a connection between reducibility in $\mathbb{Z}[[x]]$ and the existence of a p-adic root with positive valuation was established. Whereas this connection can be certainly explained in structural terms, the role of the root in the factorization process is not obvious.

Motivated by this factorization problem and the need to find explicit p-adic roots, the main goal of this paper is to provide formulas for the Hensel lifts of roots modulo p, and to give a factorization in $\mathbb{Z}[[x]]$ of certain reducible polynomials whose constant term is of the form p^w with p prime and $w > 1$. All of our formulas are given in terms of partial Bell polynomials and rely on the inversion formula of Lagrange.

On the one hand, in Section 3, we prove two versions of Hensel's lemma that give explicit formulas for the roots of any polynomial in $\mathbb{Z}_p[x]$, the ring of polynomials over the p-adic integers $\mathbb{Z}_p$. For illustration purposes, we examine the special cases of quadratic and cubic polynomials in (3.4) and (3.7), and discuss the roots of unity, providing a formula for the so-called Teichmüller lifts (see Proposition 3.9). On the other hand, we give a factorization over $\mathbb{Z}[[x]]$ for polynomials f (of degree higher than 1) with $f(0) = p^w$ that are reducible in the presence of a p-adic root in $p\mathbb{Z}_p$. Although Theorem 4.2 is formulated for polynomials, it actually holds verbatim for power series. An illustrative example is discussed at the end of Section 4.

As mentioned before, Sections 3 and 4 are related and rely on the material discussed in Section 2. For the reader's convenience, a short appendix with some of the basic properties and identities for the partial Bell polynomials is included. We finish by observing that most of the results presented here may be applied to polynomials and power series over other commutative rings.

2. Series Solutions of Algebraic Equations

The main results of this paper rely on the following consequence of the inversion formula of Lagrange for formal power series. For a detailed proof and other applications, we refer the reader to [8, Section 3.8] or [7, Section 11.6]. In what follows, $B_{n,j}(x_1, x_2, \dots)$ denotes the (n, j)-th partial Bell polynomial; see the appendix.

Lemma 2.1 (cf. [7, Corollary 11.3]). *If $\phi(t)$ is a power series of the form*

$$\phi(t) = t\bigg(1 + \sum_{r=1}^{\infty} \alpha_r \frac{t^r}{r!}\bigg),$$

then its formal inverse is given by

$$\phi^{-1}(u) = u\bigg(1 + \sum_{n=1}^{\infty} \beta_n \frac{u^n}{n!}\bigg),$$

where

$$\beta_n = \sum_{j=1}^{n} (-1)^j \frac{(n+j)!}{(n+1)!} B_{n,j}(\alpha_1, \alpha_2, \dots).$$

Inversion formulas of this type have been studied by many authors in the search for solutions of algebraic equations. For instance, a series solution for the equation $x^m + px = q$ was already given by Lambert in 1758, cf. [12]. The most general formulas we found in the literature were obtained by Birkeland around 1927. In [3], the author studied arbitrary polynomial equations and obtained explicit solutions in terms of hypergeometric functions; see also [13].

It turns out that, if $f(x)$ is a power series over a commutative ring $\mathcal{R}$ with an invertible linear coefficient, then formal series solutions for the equation $f(x) = 0$ can be obtained from Lemma 2.1 as follows.

Proposition 2.2. *Given a power series $f(x) = a_0 + a_1x + a_2x^2 + \cdots \in \mathcal{R}[[x]]$ with a_1 invertible in $\mathcal{R}$, the equation $f(x) = 0$ has the formal root*

$$x = \sum_{n=0}^{\infty} \biggl[\sum_{j=0}^{n} \frac{(-1)^{n+j+1}}{a_1^j\, n!} \frac{(n+j)!}{(n+1)!} B_{n,j}(1!a_2, 2!a_3, \dots) \biggr] \Bigl(\frac{a_0}{a_1}\Bigr)^{n+1} \tag{2.3}$$

$$= \sum_{n=0}^{\infty} \sum_{k=0}^{n} \frac{(-1)^{n-k+1}}{a_1^k\,(n+1)!} \binom{2n+1}{n-k} B_{n+k,k}(1!a_1, 2!a_2, \dots) \Bigl(\frac{a_0}{a_1}\Bigr)^{n+1}. \tag{2.4}$$

Proof. Let

$$\phi(x) = x\biggl(1 + \sum_{\ell=1}^{\infty} \alpha_\ell \frac{x^\ell}{\ell!}\biggr) \text{ with } \alpha_\ell = \ell!\, a_{\ell+1}/a_1.$$

Thus $f(x) = a_1\bigl(a_0/a_1 + \phi(x)\bigr)$ and $f(x) = 0$ if $\phi(x) = -a_0/a_1$. By Lemma 2.1, this equation has the formal root

$$\begin{aligned} x = \phi^{-1}(-a_0/a_1) &= -\frac{a_0}{a_1}\biggl(1 + \sum_{n=1}^{\infty} \frac{(-1)^n \beta_n}{n!} \Bigl(\frac{a_0}{a_1}\Bigr)^n\biggr) \\ &= -\frac{a_0}{a_1}\biggl(1 + \sum_{n=1}^{\infty} \frac{(-1)^n}{n!} \biggl[\sum_{j=1}^{n} (-1)^j \frac{(n+j)!}{(n+1)!} B_{n,j}(\alpha_1, \alpha_2, \dots)\biggr] \Bigl(\frac{a_0}{a_1}\Bigr)^n\biggr) \\ &= \sum_{n=0}^{\infty} \biggl[\sum_{j=0}^{n} \frac{(-1)^{n+j+1}}{a_1^j\, n!} \frac{(n+j)!}{(n+1)!} B_{n,j}(1!a_2, 2!a_3, \dots) \biggr] \Bigl(\frac{a_0}{a_1}\Bigr)^{n+1}, \end{aligned}$$

which gives (2.3). Now, if we set $x_j = j!a_j$, then

$$B_{n,j}(1!a_2, 2!a_3, \dots) = B_{n,j}(\tfrac{x_2}{2}\tfrac{x_3}{3}, \dots) = \frac{n!}{(n+j)!} B_{n+j,j}(0, x_2, x_3, \dots)$$

by (A.1). Moreover, by means of (A.2) and (A.3), we have

$$\begin{aligned} B_{n+j,j}(0, x_2, x_3, \dots) &= \sum_{\substack{k \le j \\ \nu \le n+j}} \binom{n+j}{\nu} B_{\nu,k}(x_1, x_2, \dots) B_{n+j-\nu, j-k}(-x_1, 0, \dots) \\ &= \sum_{k \le j} \binom{n+j}{n+k} (-x_1)^{j-k} B_{n+k,k}(x_1, x_2, \dots). \end{aligned}$$

Therefore,

$$\begin{aligned}
&\sum_{j=0}^{n} \frac{(-1)^{n+j+1}}{a_1^j\, n!} \frac{(n+j)!}{(n+1)!} B_{n,j}(1!a_2, 2!a_3, \dots) \\
&\qquad = \sum_{j=0}^{n} \frac{(-1)^{n+j+1}}{a_1^j\, (n+1)!} B_{n+j,j}(0, 2!a_2, 3!a_3, \dots) \\
&\qquad = \sum_{j=0}^{n} \sum_{k\le j} \frac{(-1)^{n-k+1}}{a_1^k\, (n+1)!} \binom{n+j}{n+k} B_{n+k,k}(1!a_1, 2!a_2, \dots) \\
&\qquad = \sum_{k=0}^{n} \frac{(-1)^{n-k+1}}{a_1^k\, (n+1)!} \Big[\sum_{j=k}^{n} \binom{n+j}{n+k} \Big] B_{n+k,k}(1!a_1, 2!a_2, \dots) \\
&\qquad = \sum_{k=0}^{n} \frac{(-1)^{n-k+1}}{a_1^k\, (n+1)!} \binom{2n+1}{n-k} B_{n+k,k}(1!a_1, 2!a_2, \dots).
\end{aligned}$$

Inserting this expression into (2.3), we arrive at (2.4). □

The simplicity (or complexity) of formulas (2.3) and (2.4) clearly depends on the structure of the partial Bell polynomials.

For example, for $x^m + px - q = 0$ with $p, q \in \mathbb{R}$, $p \neq 0$, $m > 1$, the root (2.3) takes the form

$$x = \sum_{n=0}^{\infty} \Big[\sum_{j=0}^{n} \frac{(-1)^{n+j+1}}{p^j\, n!} \frac{(n+j)!}{(n+1)!} B_{n,j}(0, \dots, (m-1)!, 0, \dots) \Big] \Big(\frac{-q}{p}\Big)^{n+1}$$

which by means of (A.3) reduces to

$$x = \sum_{k=0}^{\infty} \frac{(-1)^k}{p^k} \binom{mk}{k} \frac{1}{(m-1)k+1} \Big(\frac{q}{p}\Big)^{(m-1)k+1}. \tag{2.5}$$

This formula includes Eisenstein's series solution for $x^5 + x = q$, cf. [15],

$$x = \sum_{k=0}^{\infty} (-1)^k \binom{5k}{k} \frac{1}{4k+1} q^{4k+1}.$$

Of course, this series does not converge for all values of q, so further analysis is required to understand and possibly make sense of (2.4). While convergence in general is not the focus of this paper, we want to briefly discuss $f(x) = x^3 + x - q$ in order to illustrate a possible analytic approach. For this polynomial, the sum (2.5) becomes

$$x = \sum_{k=0}^{\infty} (-1)^k \binom{3k}{k} \frac{1}{2k+1} q^{2k+1} = q \sum_{k=0}^{\infty} \binom{3k}{k} \frac{1}{2k+1} (-q^2)^k,$$

which converges only when $q^2 \leq 4/27$. However,

$$\sum_{k=0}^{\infty} \binom{3k}{k} \frac{1}{2k+1}(-q^2)^k = {}_2F_1\left(\tfrac{1}{3}, \tfrac{2}{3}; \tfrac{3}{2}; -\tfrac{27}{4}q^2\right),$$

and since the hypergeometric function ${}_2F_1\left(\frac{1}{3}, \frac{2}{3}; \frac{3}{2}; z\right)$ extends analytically to the set $\mathbb{C} \setminus (1, \infty)$, we can actually evaluate the formal root for larger values of q. For example, if $q = 2$, then the root of $x^3 + x - 2 = 0$ provided by (2.4) is precisely $x = 2 \cdot {}_2F_1\left(\frac{1}{3}, \frac{2}{3}; \frac{3}{2}; -27\right) = 1$.

In the next section we will fully discuss the use of (2.4) to find roots of polynomials over the p-adic integers.

3. Hensel's Roots

In this section, we use Proposition 2.2 to give a version of Hensel's lemma that provides an explicit formula for the p-adic root of a polynomial in $\mathbb{Z}_p[x]$. We start by recalling some basic facts about the p-adic numbers. For a comprehensive treatment of this subject, the reader is referred to [10, 11, 14].

Let p be a prime integer. For any nonzero integer a, let $v_p(a)$ (the p-adic valuation of a) be the highest power of p which divides a, i.e., the greatest m such that $a \equiv 0 \pmod{p^m}$; we agree to write $v_p(0) = \infty$. Note that $v_p(a_1\, a_2) = v_p(a_1) + v_p(a_2)$ for all $a_1, a_2 \in \mathbb{Z}$. For any rational number $x = a/b$, define $v_p(x) = v_p(a) - v_p(b)$. Note that this expression depends only on x and not on its representation as a ratio of integers.

The p-adic norm in $\mathbb{Q}$ is defined as $\|x\|_p = p^{-v_p(x)}$ if $x \neq 0$, and $\|0\|_p = 0$. This norm is non-Archimedean; that is, $\|x + y\|_p \leq \max(\|x\|_p, \|y\|_p)$. The p-adic completion of $\mathbb{Q}$ with respect to $\|\cdot\|_p$ is denoted by $\mathbb{Q}_p$. Every $a \in \mathbb{Q}_p$ admits a unique p-adic expansion,

$$a = \frac{a_0}{p^m} + \frac{a_1}{p^{m-1}} + \cdots + \frac{a_{m-1}}{p} + a_m + a_{m+1}\, p + a_{m+2}\, p^2 + \cdots,$$

with $0 \leq a_i < p$ for all i.

We let $\mathbb{Z}_p = \{a \in \mathbb{Q}_p \,|\, \|a\|_p \leq 1\}$, the set of all numbers in $\mathbb{Q}_p$ whose p-adic expansion involves no negative powers of p. An element of $\mathbb{Z}_p$ is called a *p-adic integer*, and the set of p-adic integers is a subring of the field $\mathbb{Q}_p$. If $x \in \mathbb{Z}_p$ is such that $v_p(x) = 0$, then x is a unit and its multiplicative inverse $1/x$ is in $\mathbb{Z}_p$.

A fundamental property of the p-adic numbers is that a series in $\mathbb{Q}_p$ converges if and only if its terms approach zero. This condition is equivalent to verifying that the p-adic valuation of the terms tend to infinity.

Theorem 3.1. *Let $p > 2$ be prime and let $f(x) = a_0 + a_1x + \cdots + a_mx^m$ be a polynomial of degree m in $\mathbb{Z}_p[x]$. If $r_0 \in \mathbb{Z}$ is such that*

$$f(r_0) \equiv 0 \pmod{p} \quad \textit{and} \quad v_p(f'(r_0)) = 0,$$

then r_0 lifts to a p-adic root r of f given by

$$r = r_0 + \sum_{n=0}^{\infty} \left[\sum_{k=0}^{n} \frac{(-1)^{n-k+1}}{c_1^k\,(n+1)!} \binom{2n+1}{n-k} B_{n+k,k}(1!c_1, 2!c_2, \dots) \right] \left(\frac{c_0}{c_1}\right)^{n+1}, \tag{3.2}$$

where $c_j = \frac{f^{(j)}(r_0)}{j!}$ for $j = 0, 1, \dots, m$. Note that $v_p(c_1) = 0$ implies $1/c_1 \in \mathbb{Z}_p$.

Proof. Given $f(x)$ and $r_0 \in \mathbb{Z}$ as above, consider the function $g(x) = f(r_0 + x)$. The Taylor expansion of $g(x)$ at $x = 0$ gives

$$g(x) = f(r_0) + f'(r_0)x + \tfrac{f''(r_0)}{2!}x^2 + \cdots + \tfrac{f^{(m)}(r_0)}{m!}x^m = c_0 + c_1x + \cdots + c_mx^m,$$

with the property that $v_p(c_0) = v_p(f(r_0)) \geq 1$ and $v_p(c_1) = v_p(f'(r_0)) = 0$. Thus $c_1 \neq 0$, and by Proposition 2.2, $g(x)$ has a formal root

$$\varrho = \sum_{n=0}^{\infty} \gamma_n \frac{c_0^{n+1}}{(n+1)!},$$

where

$$\gamma_n = \sum_{k=0}^{n} \frac{(-1)^{n-k+1}}{c_1^{k+n+1}} \binom{2n+1}{n-k} B_{n+k,k}(1!c_1, 2!c_2, \dots).$$

Since $v_p(c_1) = 0$ and each $j!c_j$ is a p-adic integer, we have $\gamma_n \in \mathbb{Z}_p$ for every n. Moreover, if $n+1$ has the p-adic expansion $n+1 = n_0 + n_1p + n_2p^2 + \cdots$, we have

$$v_p((n+1)!) = \frac{n+1-s_p(n+1)}{p-1} < \frac{n+1}{p-1},$$

where $s_p(n+1) = n_0 + n_1 + n_2 + \cdots$. Therefore, since $v_p(c_0) \geq 1$, we get

$$v_p\big(\tfrac{c_0^{n+1}}{(n+1)!}\big) = v_p(c_0^{n+1}) - v_p((n+1)!) > n+1-\tfrac{n+1}{p-1} = \big(\tfrac{p-2}{p-1}\big)(n+1) \to \infty \text{ as } n \to \infty,$$

which implies that $\sum \gamma_n \frac{c_0^{n+1}}{(n+1)!}$ converges in $p\mathbb{Z}_p$. In conclusion, the formal root ϱ is indeed a p-adic root of $g(x)$ and $r_0 + \varrho \in \mathbb{Z}_p$ is a root of $f(x)$. □

More generally, we have:

Theorem 3.3. *Let $p > 2$ be prime and let $f(x) = a_0 + a_1x + \cdots + a_mx^m$ be a polynomial in $\mathbb{Z}_p[x]$. Let $\nu, \kappa \in \mathbb{Z}$ such that $0 \leq 2\kappa < \nu$. If $r_0 \in \mathbb{Z}$ is such that*

$$f(r_0) \equiv 0 \pmod{p^\nu} \quad \textit{and} \quad v_p(f'(r_0)) = \kappa,$$

then r_0 lifts to a p-adic root r of f given by

$$r = r_0 + p^{\kappa} \sum_{n=0}^{\infty} \left[\sum_{k=0}^{n} \frac{(-1)^{n-k+1}}{c_1^k\,(n+1)!} \binom{2n+1}{n-k} B_{n+k,k}(1!c_1, 2!c_2, \dots) \right] \left(\frac{c_0}{c_1}\right)^{n+1},$$

where $c_j = p^{(j-2)\kappa}\,\frac{f^{(j)}(r_0)}{j!}$ for $j = 0, 1, \dots, m$.

Proof. The proof is similar to the one for the previous theorem. Let r_0 be a root of f modulo p^{ν} and let κ be the p-adic valuation of $f'(r_0)$. Consider the function $g(x) = p^{-2\kappa} f(r_0 + p^{\kappa} x)$. A Taylor expansion of $g(x)$ at 0 gives

$$\begin{aligned} g(x) &= p^{-2\kappa} f(r_0) + p^{-\kappa} f'(r_0)x + \tfrac{f''(r_0)}{2!}x^2 + \cdots + p^{(m-2)\kappa}\,\tfrac{f^{(m)}(r_0)}{m!}x^m \\ &= c_0 + c_1 x + c_2 x^2 + \cdots + c_m x^m. \end{aligned}$$

If $0 \le 2\kappa < \nu$, then $v_p(c_0) \ge 1$ and $v_p(c_1) = 0$ since $v_p(f(r_0)) \ge \nu > 2\kappa$ and $v_p(f'(r_0)) = \kappa$. At this point, we can proceed as in the proof of Theorem 3.1 and conclude that the formal root of $g(x)$ provided by (2.4) is indeed a p-adic root of $g(x)$. If we denote that root by ϱ, then $r = r_0 + p^{\kappa}\varrho$ is a p-adic root of the polynomial $f(x)$. □

In the case of quadratic and cubic polynomials, one can use known properties of Bell polynomials to give a simpler representation of the corresponding Hensel's roots.

3.1. Quadratic Polynomials

Let $p > 2$ and $f(x) = a_0 + a_1 x + a_2 x^2 \in \mathbb{Z}_p[x]$, $a_2 \neq 0$. If there is an $r_0 \in \mathbb{Z}$ such that $f(r_0) \equiv 0 \pmod{p}$ and $v_p(f'(r_0)) = 0$, then by Theorem 3.1 and elementary Bell polynomial identities, the p-adic lift of r_0 may be written as

$$r = r_0 - \frac{c_0}{c_1} \sum_{n=0}^{\infty} \binom{2n}{n} \frac{1}{n+1} \left(\frac{c_0 c_2}{c_1^2}\right)^n \in \mathbb{Z}_p, \tag{3.4}$$

where $c_0 = f(r_0)$, $c_1 = f'(r_0)$, and $c_2 = a_2$. Note that $\binom{2n}{n}\frac{1}{n+1} \in \mathbb{Z}$ are the well-known Catalan numbers.

Example 3.5. Let us consider $f(x) = 1 + 11x - 5x^2$ over $\mathbb{Z}_7$. This polynomial has two simple roots mod 7, $r_0 = 1, 4$. Since $c_0 = f(1) = 7$, $c_1 = f'(1) = 1$, and $c_2 = -5$, the lift of $r_0 = 1$ in $\mathbb{Z}_7$ is given by

$$r = 1 - \sum_{n=0}^{\infty} \binom{2n}{n} \frac{(-5)^n}{n+1}\, 7^{n+1}.$$

On the other hand, since $f(4) = -35$ and $f'(4) = -29$, the lift of $r_0 = 4$ in $\mathbb{Z}_7$ is given by

$$r = 4 - \sum_{n=0}^{\infty} \binom{2n}{n} \frac{1}{n+1} \Big(\frac{5}{29}\Big)^{2n+1} 7^{n+1}.$$

Note that $1/29 = 1 + 3 \cdot 7 + 7^2 + 7^3 + 2 \cdot 7^4 + 5 \cdot 7^5 + O(7^6)$ is an element of $\mathbb{Z}_7$.

Example 3.6. We now consider $f(x) = 17 + 6x + 2x^2$ over $\mathbb{Z}_5$. Modulo 5 this polynomial has a double root, $r_0 = 1$. Since $f(1) = 5^2$ and $f'(1) = 2 \cdot 5$, we cannot apply any of the above theorems directly. However, the polynomial

$$g(x) = \tfrac{1}{25} f(1 + 5x) = 1 + 2x + 2x^2$$

has 1 and 3 as simple roots modulo 5, so using (3.4), we get the lifts

$$1 - \frac{5}{6} \sum_{n=0}^{\infty} \binom{2n}{n} \frac{1}{n+1} \Big(\frac{5}{18}\Big)^{n} \text{ and } 3 - \frac{25}{14} \sum_{n=0}^{\infty} \binom{2n}{n} \frac{1}{n+1} \Big(\frac{25}{98}\Big)^{n} \text{ in } \mathbb{Z}_5.$$

Therefore, the 5-adic roots of $f(x)$ are given by

$$1 + 5 - \frac{25}{6} \sum_{n=0}^{\infty} \binom{2n}{n} \frac{1}{n+1} \Big(\frac{5}{18}\Big)^{n} \text{ and } 1 + 3 \cdot 5 - \frac{125}{14} \sum_{n=0}^{\infty} \binom{2n}{n} \frac{1}{n+1} \Big(\frac{25}{98}\Big)^{n}.$$

3.2. Cubic Polynomials

Let $p > 2$ and $f(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 \in \mathbb{Z}_p[x]$, $a_3 \neq 0$. Once again, if there is an $r_0 \in \mathbb{Z}$ such that $f(r_0) \equiv 0 \pmod{p}$ and $v_p(f'(r_0)) = 0$, then Theorem 3.1 gives a formula for the p-adic lift of r_0. However, for cubic polynomials, it is more convenient to use the equation (2.3) and write the root as

$$r = r_0 + \sum_{n=0}^{\infty} \Bigg[\sum_{k=0}^{n} \frac{(-1)^{n+k+1}}{c_1^k \, n!} \frac{(n+k)!}{(n+1)!} B_{n,k}(c_2, 2c_3, 0, \dots) \Bigg] \Big(\frac{c_0}{c_1}\Big)^{n+1},$$

where $c_j = f^{(j)}(r_0)/j!$ for $j = 0, 1, 2, 3$. Note that $B_{n,k}(c_2, 2c_3, 0, \dots) = 0$ for $k < n/2$, and for $k \geq n/2$, identities (A.2) and (A.3) give

$$\begin{aligned} B_{n,k}(c_2, 2c_3, 0, \dots) &= \sum_{\substack{\kappa \leq k \\ \nu \leq n}} \binom{n}{\nu} B_{\nu,\kappa}(c_2, 0, \dots) B_{n-\nu,k-\kappa}(0, 2c_3, 0, \dots) \\ &= \sum_{\kappa \leq k} \binom{n}{\kappa} c_2^{\kappa} B_{n-\kappa,k-\kappa}(0, 2c_3, 0, \dots) \\ &= \binom{n}{2k-n} c_2^{2k-n} \frac{[2(n-k)]!}{(n-k)!} c_3^{n-k} \\ &= \frac{n!}{(2k-n)!(n-k)!} \, c_2^{2k-n} c_3^{n-k}. \end{aligned}$$

Therefore,

$$r = r_0 + \sum_{n=0}^{\infty} \Big[\sum_{k \geq n/2}^{n} \frac{(-1)^{n+k+1}}{c_1^k\, n!} \frac{(n+k)!}{(n+1)!} \frac{n!}{(2k-n)!(n-k)!}\, c_2^{2k-n} c_3^{n-k} \Big] \Big(\frac{c_0}{c_1}\Big)^{n+1},$$

and with the change $n = 2k - j$,

$$= r_0 + \frac{c_0}{c_1} \sum_{k=0}^{\infty} \Big[\sum_{j=0}^{k} \frac{(-1)^{k-j+1}}{c_1^k (2k-j+1)} \binom{k}{j} \binom{3k-j}{k} c_2^j c_3^{k-j} \Big] \Big(\frac{c_0}{c_1}\Big)^{2k-j}.$$

In summary, if r_0 is a simple root mod p of $f(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 \in \mathbb{Z}_p[x]$, then the p-adic lift of r_0 is given by

$$r = r_0 - \frac{c_0}{c_1} \sum_{k=0}^{\infty} \Big[\sum_{j=0}^{k} \frac{(-1)^{k-j} c_2^j}{2k-j+1} \binom{k}{j} \binom{3k-j}{k} \Big(\frac{c_0 c_3}{c_1}\Big)^{k-j} \Big] \Big(\frac{c_0}{c_1^2}\Big)^{k}, \tag{3.7}$$

where $c_0 = f(r_0)$, $c_1 = f'(r_0)$, $c_2 = f''(r_0)/2$, and $c_3 = a_3$.

Following the same steps as for cubic polynomials, we get the following result.

Proposition 3.8. *Let $p > 2$ and $1 < \ell < m$. Suppose $f(x) = a_0 + a_1 x + a_\ell x^\ell + a_m x^m \in \mathbb{Z}_p[x]$ is such that $p \,|\, f(0)$ but $p \nmid f'(0)$. Then $r_0 = 0$ lifts to a p-adic root of f given by*

$$r = -\frac{a_0}{a_1} \sum_{k=0}^{\infty} \Big[\sum_{j=0}^{k} \tfrac{(-1)^{m(k-j)+\ell j}\, a_\ell^j}{m(k-j)+\ell j-k+1} \binom{k}{j} \binom{m(k-j)+\ell j}{k} \Big(\frac{a_0^{m-\ell} a_m}{a_1^{m-\ell}}\Big)^{k-j} \Big] \Big(\frac{a_0^{\ell-1}}{a_1^{\ell}}\Big)^{k}.$$

3.3. Roots of Unity

Let $p > 2$ and $f(x) = x^m - 1$. Assume that r_0 is a single root mod p of f. Then r_0 lifts to a p-adic root of the form (3.2) with $c_0 = r_0^m - 1$ and $c_j = \binom{m}{j} r_0^{m-j}$ for $j = 1, \ldots, m$. Now, since

$$j! c_j = r_0^{m-j} (m)_j \;\text{ with }\; (m)_j = \frac{m!}{(m-j)!},$$

homogeneity properties of the Bell polynomials together with identity (A.4) give

$$\begin{aligned} B_{n+k,k}(1!c_1, 2!c_2, \ldots) &= B_{n+k,k}(r_0^{m-1}(m)_1, r_0^{m-2}(m)_2, \ldots) \\ &= r_0^{mk-(n+k)} B_{n+k,k}((m)_1, (m)_2, \ldots) \\ &= r_0^{mk-(n+k)} \frac{1}{k!} \sum_{j=0}^{k} (-1)^{k-j} \binom{k}{j} (jm)_{n+k}. \end{aligned}$$

Therefore,

$$\sum_{k=0}^{n}\frac{(-1)^{n-k+1}}{c_1^k\,(n+1)!}\binom{2n+1}{n-k}B_{n+k,k}(1!c_1,2!c_2,\dots)$$
$$=\sum_{k=0}^{n}\frac{(-1)^{n-k+1}}{(r_0^{m-1}m)^k\,(n+1)!}\binom{2n+1}{n-k}r_0^{mk-(n+k)}\frac{1}{k!}\sum_{j=0}^{k}(-1)^{k-j}\binom{k}{j}(jm)_{n+k}$$
$$=\sum_{k=0}^{n}\sum_{j=0}^{k}\frac{(-1)^{n-j+1}}{r_0^n\,m^k\,(n+1)!}\binom{2n+1}{n-k}\frac{1}{k!}\binom{k}{j}(jm)_{n+k}.$$

Finally, the p-adic lift of r_0 is given by

$$r=r_0-\frac{c_0}{c_1}\sum_{n=0}^{\infty}\left[\sum_{k=0}^{n}\sum_{j=0}^{k}\frac{(-1)^{n-j}}{m^k\,(n+1)!}\binom{2n+1}{n-k}\frac{1}{k!}\binom{k}{j}(jm)_{n+k}\right]\left(\frac{c_0}{r_0c_1}\right)^n,$$

where $c_0=f(r_0)$ and $c_1=f'(r_0)$.

For $m=p-1$, the above expression gives an explicit formula for the Teichmüller lifts.

Proposition 3.9. *Let $p>2$. Every integer $q\in\{1,\dots,p-1\}$ is a $(p-1)$-st root of unity mod p and lifts to a p-adic root of unity ξ_q given by*

$$\xi_q=q-\frac{c_0}{c_1}\sum_{n=0}^{\infty}\left[\sum_{k=0}^{n}\sum_{j=0}^{k}\frac{(-1)^{n-j}}{(p-1)^k\,(n+1)!}\binom{2n+1}{n-k}\frac{1}{k!}\binom{k}{j}(j(p-1))_{n+k}\right]\left(\frac{c_0}{qc_1}\right)^n,$$

where $c_0=q^{p-1}-1$ and $c_1=(p-1)q^{p-2}$.

4. Factorization of Polynomials over $\mathbb{Z}[[x]]$

Let $f(x)=f_0+f_1x+f_2x^2+\cdots$ be a formal power series in $\mathbb{Z}[[x]]$. It is easy to prove that $f(x)$ is invertible in $\mathbb{Z}[[x]]$ if and only if $|f_0|=1$. A natural question, initially discussed in [4], is whether or not a non-invertible element of $\mathbb{Z}[[x]]$ can be factored over $\mathbb{Z}[[x]]$. In recent years, this question has been investigated by several authors, leading to sufficient and in some cases necessary reducibility criteria; see e.g., [2, 5, 9]. In particular, [9] deals with the factorization of formal power series over principal ideal domains.

For the case at hand, the following elementary results are known. The formal power series $f(x)=f_0+f_1x+f_2x^2+\cdots$ is irreducible in $\mathbb{Z}[[x]]$ if $|f_0|$ is prime, or if $|f_0|=p^w$ with p prime, $w\in\mathbb{N}$, and $\gcd(p,f_1)=1$.

On the other hand, if f_0 is neither a unit nor a prime power, then $f(x)$ is reducible. In this case, the factorization algorithm is simple and relies on a recursion and a single diophantine equation; see [4, Prop. 3.4].

Finally, in the remaining case when f_0 is a prime power and f_1 is divisible by p, the reducibility of $f(x)$ in $\mathbb{Z}[[x]]$ is linked to the existence of a p-adic root of positive valuation. The goal of this section is to give an explicit factorization over $\mathbb{Z}[[x]]$ for reducible polynomials of the form

$$f(x) = p^w + p^m\gamma_1 x + \gamma_2 x^2 + \cdots + \gamma_d x^d, \quad m \geq 1,\ w \geq 2,\ d \geq 2, \tag{4.1}$$

where $\gamma_1, \ldots, \gamma_d \in \mathbb{Z}$ and $\gcd(p, \gamma_1) = 1$. This is the only type of polynomial for which the reducibility and factorization over $\mathbb{Z}[[x]]$ is not straightforward.

Theorem 4.2. *Let p be an odd prime and let f be a polynomial of the form* (4.1). *Assume that f has a simple root $r \in p\mathbb{Z}_p$ with $v_p(r) = \ell \leq m$ and $r = p^\ell(1 + \sum_{j=1}^{\infty} e_j p^{\ell j})$ with $e_j \in \mathbb{Z}$. Then $f(x)$ admits the factorization*

$$f(x) = \left(p^\ell - x - x\sum_{n=1}^{\infty} a_n x^n\right)\left(p^{w-\ell} + (p^{w-2\ell} + p^{m-\ell}\gamma_1)x + x\sum_{n=1}^{\infty} b_n x^n\right),$$

where the coefficients a_n are given by (4.4), *and $b_n = \hat{b}_n/p^{\ell n}$ with $\hat{b}_n$ as in* (4.11).

Remark. (a) As shown in Lemma 4.12, $\hat{b}_n$ is divisible by $p^{\ell n}$, so $b_n \in \mathbb{Z}$ for all n.

(b) If $r \in p\mathbb{Z}_p$ is a root of f with $v_p(r) = \ell \leq m$, then $2\ell \leq w$.

(c) If $w \leq 2m$ and f has a root $r \in p\mathbb{Z}_p$, then $v_p(r) = \ell \leq m$ holds. If $w > 2m$, then 0 lifts to a p-adic root of f, but it is not necessarily true that f has a root of valuation less than or equal to m. This property depends on the coefficients $\gamma_2, \gamma_3, \ldots$. However, even if that condition fails, $f(x)$ is still reducible and a factorization can be obtained through the algorithm given in [5, Prop. 2.4].

(d) A p-adic integer r with $v_p(r) = \ell$ can always be written as $r = p^\ell(e_0 + \sum_{j=1}^{\infty} e_j p^{\ell j})$ with $e_0 \in \mathbb{Z}_p^*$. For factorization purposes, we can assume without loss of generality $e_0 = 1$. Otherwise, consider $g(x) = f(x/e_0^*)$, where e_0^* is such that $e_0 e_0^* = 1 \pmod{p^\ell}$.

(e) As discussed in [5], the existence of a root in $p\mathbb{Z}_p$ is in many cases (e.g., when $d \leq 3$) a necessary condition for the polynomial (4.1) to factor over $\mathbb{Z}[[x]]$.

Remark. If f has a multiple root in $p\mathbb{Z}_p$, then $f(x)$ admits the simpler factorization

$$f(x) = G(x) f_{\mathrm{red}}(x),$$

where $G(x) = \gcd(f(x), f'(x)) \in \mathbb{Z}[x]$ and $f_{\mathrm{red}}(x) = f(x)/G(x)$.

Proof of Theorem 4.2

Let $r = p^{\ell}\big(1 + \sum_{j=1}^{\infty} e_j p^{\ell j}\big)$ be the p-adic root of f and define

$$\phi(x) = xE(x) \quad \text{with} \quad E(x) = 1 + \sum_{j=1}^{\infty} e_j x^j. \tag{4.3}$$

Thus $r = \phi(p^{\ell})$ in $\mathbb{Z}_p$ and therefore $p^{\ell} = \phi^{-1}(r)$. Define $A(x) = p^{\ell} - \phi^{-1}(x)$. So $A(r) = 0$ in $\mathbb{Z}_p$, and by Lemma 2.1, we have

$$A(x) = p^{\ell} - \phi^{-1}(x) = p^{\ell} - x\Big(1 + \sum_{n=1}^{\infty} a_n x^n\Big),$$

where

$$a_n = \frac{1}{n!}\sum_{k=1}^{n}(-1)^k \frac{(n+k)!}{(n+1)!} B_{n,k}(1!e_1, 2!e_2, \dots) \in \mathbb{Z}. \tag{4.4}$$

Our goal is to find $B(x) \in \mathbb{Z}[[x]]$ such that $f(x) = A(x)B(x)$. For convenience, consider

$$\hat{f}(x) = p^{-2\ell} f(p^{\ell}x) \quad \text{and} \quad \hat{A}(x) = p^{-\ell} A(p^{\ell}x).$$

Thus

$$\hat{A}(x) = 1 - x - x\sum_{n=1}^{\infty} p^{\ell n} a_n x^n.$$

Proposition 4.5. *The reciprocal of $\hat{A}(x)$ is a power series in $\mathbb{Z}[[x]]$ of the form*

$$\hat{A}(x)^{-1} = \frac{1}{\hat{A}(x)} = 1 + x + x\sum_{n=1}^{\infty} t_n x^n$$

with

$$t_n = 1 + \sum_{k=1}^{n} p^{\ell k}\, \frac{n+1-k}{k!} \sum_{j=1}^{k}(-1)^j \frac{(n+j)!}{(n+1)!} B_{k,j}(1!e_1, 2!e_2, \dots) \in \mathbb{Z}. \tag{4.6}$$

Proof. As an application of Faà di Bruno's formula (cf. Thm. B in [8, Section 3.5]),

and using basic properties of partial Bell polynomials, we have

$$\begin{aligned}
\hat{A}(x)^{-1} &= 1 + x + \sum_{n=2}^{\infty}\sum_{k=1}^{n} \frac{k!}{n!} B_{n,k}(1, 2!a_1p^{\ell}, 3!a_2p^{2\ell}, \dots)\, x^n \\
&= 1 + x + \sum_{n=2}^{\infty}\sum_{k=1}^{n} k! \left[\sum_{j=0}^{k} \frac{n!}{(n-k)!j!} B_{n-k,k-j}(1!p^{\ell}a_1, 2!p^{2\ell}a_2, \dots)\right] \frac{x^n}{n!} \\
&= 1 + x + \sum_{n=1}^{\infty} \left[1 + \sum_{k=1}^{n} \left[\sum_{j=1}^{n+1-k} \tfrac{(n+1-k)!}{k!(n+1-k-j)!} p^{\ell k} B_{k,j}(1!a_1, 2!a_2, \dots)\right]\right] x^{n+1} \\
&= 1 + x + x\sum_{n=1}^{\infty} \left[1 + \sum_{k=1}^{n} \frac{p^{\ell k}}{k!} \left[\sum_{j=1}^{k} \tbinom{n+1-k}{j} j!\, B_{k,j}(1!a_1, 2!a_2, \dots)\right]\right] x^n.
\end{aligned}$$

Thus

$$\begin{aligned}
t_n &= 1 + \sum_{k=1}^{n} \frac{p^{\ell k}}{k!} \sum_{j=1}^{k} \binom{n+1-k}{j} j!\, B_{k,j}(1!a_1, 2!a_2, \dots) \\
&= 1 + \sum_{k=1}^{n} p^{\ell k}\, \frac{n+1-k}{k!} \sum_{j=1}^{k} \binom{n-k}{j-1} (j-1)! B_{k,j}(1!a_1, 2!a_2, \dots)
\end{aligned}$$

Now, if we write $k!a_k$ as

$$k!a_k = \sum_{j=1}^{k} \binom{k+j}{j-1} (j-1)! B_{k,j}(-1!e_1, -2!e_2, \dots),$$

then by means of Theorem 15 in [6] we get

$$\begin{aligned}
&\sum_{j=1}^{k} \binom{n-k}{j-1} (j-1)! B_{k,j}(1!a_1, 2!a_2, \dots) \\
&\qquad = \sum_{j=1}^{k} \binom{n+j}{j-1} (j-1)! B_{k,j}(-1!e_1, -2!e_2, \dots) \\
&\qquad = \sum_{j=1}^{k} (-1)^j \frac{(n+j)!}{(n+1)!} B_{k,j}(1!e_1, 2!e_2, \dots).
\end{aligned}$$

In other words, t_n has the form claimed in (4.6). □

Now, motivated by (4.6), for $n \geq 1$ we consider

$$T_n(x) = 1 + \sum_{k=1}^{\infty} \frac{n+1-k}{k!} \left[\sum_{j=1}^{k} (-1)^j \frac{(n+j)!}{(n+1)!} B_{k,j}(1!e_1, 2!e_2, \dots)\right] x^k.$$

Lemma 4.7. *With $E(x)$ as in (4.3), we have*

$$T_n(x) = E(x)^{-n-2}\big(E(x) + xE'(x)\big).$$

Proof. Fix $n \geq 1$ and denote

$$\tau_k = \frac{1}{k!}\sum_{j=1}^{k}(-1)^j \frac{(n+j)!}{n!} B_{k,j}(1!e_1, 2!e_2, \dots).$$

Then

$$T_n(x) = 1 + \sum_{k=1}^{\infty}\Big(1 - \frac{k}{n+1}\Big)\tau_k x^k = 1 + \sum_{k=1}^{\infty}\tau_k x^k - \frac{1}{n+1}\sum_{k=1}^{\infty} k\tau_k x^k.$$

Using again Theorem B in [8, Sec. 3.5], it follows that $1 + \sum_{k=1}^{\infty}\tau_k x^k = E(x)^{-n-1}$. Therefore,

$$\begin{aligned} T_n(x) &= E(x)^{-n-1} - \frac{1}{n+1}x\frac{d}{dx}\Big(E(x)^{-n-1}\Big) \\ &= E(x)^{-n-1} + xE(x)^{-n-2}E'(x) = E(x)^{-n-2}\big(E(x) + xE'(x)\big). \end{aligned}$$

□

As a direct consequence of this lemma we get the recurrence relation

$$T_{n-1}(x) = E(x)T_n(x),$$

which can be used to define $T_0(x)$ and $T_{-n}(x)$ for $n \geq 1$. More precisely, we let

$$T_0(x) = E(x)T_1(x) \text{ and } T_{-n}(x) = E(x)^{n+1}T_1(x) \text{ for } n \geq 1.$$

Given that

$$\hat{f}(x) = p^{-2\ell}f(p^\ell x) = p^{w-2\ell} + p^{m-\ell}\gamma_1 x + \sum_{n=2}^{d} p^{\ell(n-2)}\gamma_n x^n, \tag{4.8}$$

the relation $T_{n-j}(x) = E(x)^j T_n(x)$ gives

$$p^{w-2\ell}T_n(x) + p^{m-\ell}\gamma_1 T_{n-1}(x) + \sum_{j=2}^{d} p^{\ell(j-2)}\gamma_j T_{n-j}(x) = \hat{f}(E(x))T_n(x). \tag{4.9}$$

Moreover, since $E(x)$ is a unit in $\mathbb{Z}[[x]]$, for every $\nu \in \mathbb{Z}$ the function $T_\nu(x)$ is in $\mathbb{Z}[[x]]$ and so $T_\nu(p^\ell) \in \mathbb{Z}_p$.

Lemma 4.10. *For $\nu \geq -1$, the p-adic numbers $T_\nu(p^\ell)$ satisfy*

$$T_\nu(p^\ell) - t_\nu \equiv 0 \pmod{p^{\ell(\nu+2)}}$$

with t_ν as in (4.6) for $\nu > 0$ and $t_0 = t_{-1} = 1$.

Proof. For $\nu = n \geq 1$ the statement is a consequence of the fact that t_n is the n-th partial sum of $T_n(p^\ell)$ and the coefficient of x^{n+1} in $T_n(x)$ is zero. Further, given that

$$E(p^\ell) = 1 + p^\ell e_1 + O(p^{2\ell}) \text{ and } T_1(p^\ell) = 1 - p^\ell e_1 + O(p^{2\ell}),$$

we have

$$T_0(p^\ell) = \big(1 + p^\ell e_1 + O(p^{2\ell})\big)\big(1 - p^\ell e_1 + O(p^{2\ell})\big) \equiv 1 \pmod{p^{2\ell}}.$$

This implies $T_0(p^\ell) - t_0 \equiv 0 \pmod{p^{2\ell}}$. Finally, since $T_{-1}(p^\ell) = E(p^\ell)^2 T_1(p^\ell)$, and because $E(p^\ell)^2$ and $T_1(p^\ell)$ are both of the form $1 + O(p^\ell)$, we get $T_{-1}(p^\ell) \equiv 1 \pmod{p^\ell}$. Hence $T_{-1}(p^\ell) - t_{-1} \equiv 0 \pmod{p^\ell}$. □

Using $\hat{f}(x)$ as in (4.8), we now define

$$\begin{aligned}\hat{B}(x) &= \hat{f}(x)\hat{A}(x)^{-1} \\ &= \Big(p^{w-2\ell} + p^{m-\ell}\gamma_1 x + \sum_{n=2}^{d} p^{\ell(n-2)}\gamma_n x^n\Big)\Big(1 + x + x\sum_{n=1}^{\infty} t_n x^n\Big),\end{aligned}$$

and write it as

$$\hat{B}(x) = p^{w-2\ell} + (p^{w-2\ell} + p^{m-\ell}\gamma_1)x + x\sum_{n=1}^{\infty} \hat{b}_n x^n$$

with

$$\hat{b}_n = p^{w-2\ell}t_n + p^{m-\ell}\gamma_1 t_{n-1} + \sum_{j=2}^{d} p^{\ell(j-2)}\gamma_j t_{n-j} \in \mathbb{Z}, \tag{4.11}$$

where t_n is given by (4.6), $t_0 = t_{-1} = 1$, and $t_{-n} = 0$ for $n > 1$.

Lemma 4.12. *The coefficients $\hat{b}_n$ are divisible by $p^{\ell n}$.*

Proof. First of all, since $p^{-\ell}r = E(p^\ell)$ is a p-adic root of $\hat{f}$, identity (4.9) implies

$$p^{w-2\ell}T_n(p^\ell) + p^{m-\ell}\gamma_1 T_{n-1}(p^\ell) + \sum_{j=2}^{d} p^{\ell(j-2)}\gamma_j T_{n-j}(p^\ell) = 0 \text{ in } \mathbb{Z}_p.$$

Therefore, for $n \geq d-1$,

$$\begin{aligned}\hat{b}_n &= p^{w-2\ell}t_n + p^{m-\ell}\gamma_1 t_{n-1} + \sum_{j=2}^{d} p^{\ell(j-2)}\gamma_j t_{n-j} \\ &= p^{w-2\ell}\big(t_n - T_n(p^\ell)\big) + p^{m-\ell}\gamma_1\big(t_{n-1} - T_{n-1}(p^\ell)\big) \\ &\qquad + \sum_{j=2}^{d} p^{\ell(j-2)}\gamma_j\big(t_{n-j} - T_{n-j}(p^\ell)\big),\end{aligned}$$

which by Lemma 4.10 is congruent to 0 modulo $p^{\ell n}$. Similarly, for $1 \le n < d-1$,

$$\begin{aligned}\hat{b}_n &= p^{w-2\ell}t_n + p^{m-\ell}\gamma_1 t_{n-1} + \sum_{j=2}^{n+1} p^{\ell(j-2)}\gamma_j t_{n-j} \\ &\equiv -\sum_{j=n+2}^{d} p^{\ell(j-2)}\gamma_j T_{n-j}(p^\ell) \equiv 0 \pmod{p^{\ell n}}.\end{aligned}$$

□

Finally, defining $B(x) = p^\ell \hat{B}(x/p^\ell)$, we arrive at the factorization $f(x) = A(x)B(x)$.

Remark. It is worth mentioning that our method for factorization in $\mathbb{Z}[[x]]$ is not restricted to polynomials and can be applied to power series. As an example, consider

$$f(x) = 9 + 12x + 7x^2 + 8x^3 \sum_{k=0}^{\infty} x^k = 9 + 12x + 7x^2 + \frac{8x^3}{1-x},$$

discussed by Bézivin in [2]. This series is reducible in $\mathbb{Z}[[x]]$ and factors as

$$f(x) = \frac{(3-x)^2(1+x)}{1-x}.$$

The reader is invited to confirm that the power series version of Theorem 4.2 gives the factorization $f(x) = A(x)B(x)$ with $A(x) = 3 - x$ and $B(x) = \frac{(3-x)(1+x)}{1-x}$.

An interesting feature of this example is that the partial sums $f_d(x) = 9 + 12x + 7x^2 + \cdots + 8x^d$ of $f(x)$ of degree $d \ge 2$ are all irreducible in $\mathbb{Z}[[x]]$. This was proved in [2, Prop. 8.1], but it can also be derived from Proposition 3.4 of [6] together with the observation that for $d \ge 2$, the polynomial $f_d(x)$ has no roots in $p\mathbb{Z}_p$.

References

[1] E.T. Bell, *Exponential polynomials*, Ann. of Math., **35** (1934), pp. 258–277.

[2] J.-P. Bézivin, *Factorisation de polynômes*, unpublished manuscript (in French), 2008, available at http://jp.bezivin.pagesperso-orange.fr/

[3] R. Birkeland, *Über die Auflösung algebraischer Gleichungen durch hypergeometrische Funktionen*, Math. Z. **26** (1927), no. 1, 566–578.

[4] D. Birmajer and J.B. Gil, *Arithmetic in the ring of formal power series with integer coefficients*, Amer. Math. Monthly **115** (2008), no. 6, 541–549.

[5] D. Birmajer, J.B. Gil, and M.D. Weiner, *Factoring polynomials in the ring of formal power series over* $\mathbb{Z}$, Int. J. Number Theory **8** (2012), no. 7, 1763–1776.

[6] D. Birmajer, J.B. Gil, and M.D. Weiner, *Some convolution identities and an inverse relation involving partial Bell polynomials*, Electron. J. Combin. **19** (2012), no. 4, Paper 34, 14 pp.

[7] C.A. Charalambides, *Enumerative Combinatorics*, Chapman and Hall/CRC, Boca Raton, 2002.

[8] L. Comtet, *Advanced Combinatorics: The Art of Finite and Infinite Expansions*, D. Reidel Publishing Co., Dordrecht, 1974.

[9] J. Elliott, *Factoring formal power series over principal ideal domains*, preprint, arXiv:1107.4860v4 [math.AC], 2011.

[10] S. Katok, *p-adic Analysis Compared with Real*, Mathematics Advanced Study Semesters (Student Mathematical Library, 37), American Mathematical Society, Providence, RI, 2007.

[11] N. Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, 2nd edition, Grad. Texts in Math. 58, Springer, New York, 1984.

[12] J.H. Lambert, *Observationes variae in Mathesin puram.*, Acta Helvetica **3** (1758), 128–168.

[13] M. Passare and A. Tsikh, *Algebraic equations and hypergeometric series*, in The legacy of Niels Henrik Abel, 653–672, Springer, Berlin, 2004.

[14] J.-P. Serre, *A Course in Arithmetic*, Grad. Texts in Math. 7, Springer, New York, 1973.

[15] J. Stillwell, *Eisenstein's footnote*, Math. Intelligencer **17** (1995), no. 2, 58–62.

[16] W. Wang and T. Wang, *General identities on Bell polynomials*, Comput. Math. Appl. **58** (2009), no. 1, 104–118.

Appendix: Some Properties of Bell Polynomials

Throughout this paper, we make extensive use of the well-known partial Bell polynomials. For any sequence $x_1, x_2, \dots$, the (n,k)-th partial Bell polynomial is defined by

$$B_{n,k}(x) = \sum_{i \in \pi(n,k)} \frac{n!}{i_1! i_2! \cdots} \left(\frac{x_1}{1!}\right)^{i_1} \left(\frac{x_2}{2!}\right)^{i_2} \cdots,$$

where $\pi(n,k)$ is the set of all sequences $i = (i_1, i_2, \dots)$ of nonnegative integers such that

$$i_1 + i_2 + \cdots = k \quad \text{and} \quad i_1 + 2i_2 + 3i_3 + \cdots = n.$$

Clearly, these polynomials satisfy the homogeneity relation

$$B_{n,k}(abx_1, ab^2x_2, ab^3x_3, \dots) = a^k b^n B_{n,k}(x_1, x_2, x_3, \dots).$$

Here are other elementary identities (cf. [8, Section 3.3]) needed in this paper:

$$B_{n,k}(\tfrac{x_2}{2}, \tfrac{x_3}{3}, \dots) = \frac{n!}{(n+k)!} B_{n+k,k}(0, x_2, x_3, \dots), \tag{A.1}$$

$$B_{n,k}(x_1 + x_1', x_2 + x_2', \dots) = \sum_{\substack{\kappa \le k \\ \nu \le n}} \binom{n}{\nu} B_{\nu,\kappa}(x_1, x_2, \dots) B_{n-\nu,k-\kappa}(x_1', x_2', \dots), \tag{A.2}$$

$$B_{n,k}(0, \dots, 0, x_j, 0, \dots) = 0, \text{ except } B_{jk,k} = \frac{(jk)!}{k!(j!)^k}\, x_j^k. \tag{A.3}$$

Also of special interest is the identity

$$B_{n,k}((a)_1, (a)_2, \dots) = \frac{1}{k!} \sum_{j=0}^{k} (-1)^{k-j} \binom{k}{j} (ja)_n, \tag{A.4}$$

where $(a)_n = a(a-1)\cdots(a-n+1)$. This is a special case of [16, Example 3.2].

For more on Bell polynomials and their applications, see, e.g., [1, 7, 8, 16].