Criteria for the integrality of nth roots of power series

John Pomerat & Armin Straub
University of South Alabama

June 17, 2024

Abstract

Heninger, Rains and Sloane raised the question of which power series with integer coefficients can be written as the nth power of another power series with integer coefficients and constant term 1. We provide necessary and sufficient conditions, as well as compare with a general integrality criterion due to Dieudonné and Dwork that can be applied to this question as well.

1 Introduction

Heninger, Rains and Sloane [HRS06] raise and investigate the question of charactizing when a formal power series $f(x) \in 1 + x\mathbb{Z}[[x]]$ has an nth root $g(x) \in 1 + x\mathbb{Z}[[x]]$. That is, given $f(x)$, does there exist $g(x) \in 1 + x\mathbb{Z}[[x]]$ such that $f(x) = g(x)^n$? Among other results, a necessary condition is proved in [HRS06, Theorem 16] in the case where n is a prime. In the following, we extend this condition to the case of prime powers and prove that it is not only necessary but also sufficient. As explained below, the case of general n can be reduced to the case of prime powers so that Theorem 1.1 can be considered an answer to the question of Heninger, Rains and Sloane.

Theorem 1.1. *Let $a_1, a_2, \ldots \in \mathbb{Z}_p$ and $r \in \mathbb{Z}_{>0}$. The power series $(1+a_1x+a_2x^2+\ldots)^{1/p^r}$ has p-integral coefficients if and only if*

$$1 + a_1x + a_2x^2 + \ldots \equiv (1 + a_{p^r}x + a_{2p^r}x^2 + \ldots)^{p^r} \pmod{p^{r+1}}. \tag{1}$$

Here, as well as throughout, p denotes a prime. We write $\mathbb{Z}_p$ for the ring of p-adic integers as well as $\mathbb{Q}_p$ for its fraction field (for nice introductions to p-adic numbers, we refer to [Kob84] and [Rob00]). For $A, B \in \mathbb{Q}_p[[x]]$, we will write either $A \equiv B \pmod{p^r\mathbb{Z}_p[[x]]}$ or, more succinctly, $A \equiv B \pmod{p^r}$ to mean that $A - B \in p^r\mathbb{Z}_p[[x]]$. Since $\mathbb{Z}$ and $\mathbb{Q}$ naturally embed into $\mathbb{Z}_p$ and $\mathbb{Q}_p$, we may without possible confusion treat them as subsets. For instance, given $a \in \mathbb{Q}$, we say that $a \in \mathbb{Z}_p$ if and only if the (reduced) denominator of a is not a multiple of p.

As reviewed in Section 2, if $f(x) = g(x)^n$ for two power series $f(x), g(x)$ in $1 + x\mathbb{Q}[[x]]$, then we necessarily have $g(x) = f(x)^{1/n}$ where $f(x)^{1/n}$ is well-defined as a power series by the binomial expansion (5). A more general (but ultimately equivalent) version of the question by Heninger, Rains and Sloane therefore is to ask: under which conditions on $f(x) \in 1 + x\mathbb{Z}[[x]]$ and $\lambda \in \mathbb{Q}$ has the power series $f(x)^\lambda$ integral coefficients itself? This question for rational exponents λ readily reduces to the question for $\lambda = 1/p^r$ where p^r is a prime power (and this is the case covered by Theorem 1.1).

Proposition 1.2. *Suppose $f(x) \in 1 + x\mathbb{Z}[[x]]$ and $\lambda \in \mathbb{Q}$. Write $\lambda = n/(p_1^{r_1} \cdots p_m^{r_m})$, where $r_j \in \mathbb{Z}_{>0}$ and where the p_j are distinct primes not dividing $n \in \mathbb{Z}$. Then we have $f(x)^\lambda \in \mathbb{Z}[[x]]$ if and only if $f(x)^{1/p^r} \in \mathbb{Z}_p[[x]]$ for all $p^r \in \{p_1^{r_1}, \dots, p_m^{r_m}\}$.*

Proof. Observe that $f(x)^\lambda \in \mathbb{Z}[[x]]$ if and only if $f(x)^\lambda \in \mathbb{Z}_p[[x]]$ for all primes p. If p is a prime not dividing the denominator of λ, then $\lambda \in \mathbb{Z}_p$ and it follows readily that $f(x)^\lambda \in \mathbb{Z}_p[[x]]$ (see the discussion after the binomial expansion (5)). On the other hand, suppose that $p^r \in \{p_1^{r_1}, \dots, p_m^{r_m}\}$. Then, as reviewed in Section 2, $f(x)^\lambda \in \mathbb{Z}_p[[x]]$ if and only if $f(x)^{\lambda\mu} = f(x)^{1/p^r} \in \mathbb{Z}_p[[x]]$ where $\mu = 1/(p^r\lambda) \in \mathbb{Z}_p^\times$. $\square$

Our criterion for the p-integrality of power series $f(x)^{1/p^r}$ proved in Theorem 1.1 is particularly easy to use for certain basic applications, such as the ones illustrated in the examples below.

Example 1.3. As a first, particularly simple application of Theorem 1.1, let us confirm that the power series

$$(1 - 12x + 12x^2 + 8x^3)^{-1/6} = 1 + 2x + 12x^2 + 92x^3 + 784x^4 + 7056x^5 + \dots \qquad (2)$$

has integer coefficients. By Proposition 1.2, this is the case if and only if $f(x)^{1/p} \in \mathbb{Z}_p[[x]]$ for $p \in \{2, 3\}$ where $f(x) = 1 - 12x + 12x^2 + 8x^3$. In the case $p = 2$, by Theorem 1.1, we have $f(x)^{1/2} \in \mathbb{Z}_2[[x]]$ if and only if $f(x) \equiv (1 + 12x)^2 \pmod 4$, which is clearly true. Likewise, $f(x)^{1/3} \in \mathbb{Z}_3[[x]]$ if and only if $f(x) \equiv (1 + 8x)^3 \pmod 9$, which is true as well. On the other hand, the same analysis shows that, for instance, $(1 - 12x + 12x^2 - 8x^3)^{-1/6}$ does not have coefficients that are all integers (indeed, the coefficient of x^3 is $284/3$).

Example 1.4. It follows from Theorem 1.1 that, if $a_1, a_2, \dots, a_d \in \mathbb{Z}_p$ with $d < p^r$, then $(1 + a_1x + a_2x^2 + \dots + a_dx^d)^{1/p^r} \in \mathbb{Z}_p[[x]]$ if and only if $a_1, a_2, \dots, a_d \in p^{r+1}\mathbb{Z}_p$. In particular, $(1 + ax)^{1/p^r} \in \mathbb{Z}_p[[x]]$ if and only if $a \in p^{r+1}\mathbb{Z}_p$.

Example 1.5. The coefficients $c(n, k)$ in the power series expansions

$$\sum_{n=0}^{\infty} c(n, k)x^n = (1 - k^2x)^{-1/k}$$

are studied in [SMA09]. These numbers are referred to as k-central binomial coefficients, with $c(n,2) = \binom{2n}{n}$ the usual central binomial coefficients. It follows from the binomial theorem, see [SMA09, Proposition 2.1], that

$$c(n,k) = (-1)^n \binom{-1/k}{n} k^{2n} = \frac{k^n}{n!} \prod_{m=1}^{n-1} (1+km).$$

In [SMA09, Theorem 2.2], these coefficients are proved to be positive integers. For instance, in the case $k=4$, this proves that $(1-16x)^{-1/4} \in \mathbb{Z}[[x]]$. This, however, is not best possible in the sense that, already, $(1-8x)^{-1/4} \in \mathbb{Z}[[x]]$ (this observation is equivalent to the fact that 2^n divides $c(n,4)$). More generally, we find, as an application of Theorem 1.1, that, for any nonzero $k \in \mathbb{Z}$,

$$(1 - k\,\mathrm{rad}(k)x)^{-1/k} \in \mathbb{Z}[[x]], \tag{3}$$

where $\mathrm{rad}(k)$ denotes the largest squarefree integer dividing k (for instance, $\mathrm{rad}(4) = 2$ and $\mathrm{rad}(24) = 6$). The result (3) is a strengthening of [SMA09, Theorem 2.2] and follows directly from the observation made in the previous example that $(1+ax)^{1/p^r} \in \mathbb{Z}_p[[x]]$ if and only if $a \in p^{r+1}\mathbb{Z}_p$. Moreover, it follows from Theorem 1.1 combined with Proposition 1.2 that (3) is strongest possible in the sense that, with the exponent $-1/k$ fixed, $(1-ax)^{-1/k} \in \mathbb{Z}[[x]]$ if and only if a is a multiple of $k\,\mathrm{rad}(k)$.

Example 1.6. Suppose that $f(x) \in 1 + x\mathbb{Z}[[x]]$ and $n \in \mathbb{Z}_{>0}$. Heninger, Rains and Sloane proved [HRS06, Theorem 1] that the power series $f(x)^{1/n}$ has integer coefficients if and only if this is true for $f(x)$ with its coefficients reduced modulo $n\,\mathrm{rad}(n)$. As in the previous example, this result can be deduced as a corollary of Theorem 1.1.

Example 1.7. For $a, b, c \in \mathbb{Z}$, Noe [Noe06] studies the generalized trinomial coefficients

$$T_n(a,b,c) = [x^n](a + bx + cx^2)^n,$$

where $[x^n]f(x)$ denotes the coefficient of x^n in $f(x)$, and notes that they have the ordinary generating function

$$\sum_{n \geq 0} T_n(a,b,c)x^n = \frac{1}{\sqrt{1 - 2bx + dx^2}} \tag{4}$$

where $d = b^2 - 4ac$ (note that $T_n(a,b,c)$ only depends on ac, not on the individual values of a and c). As an application of Theorem 1.1, we can conclude that these are the only instances in which the power series $(1+\alpha x+\beta x^2)^{-1/2}$, with $\alpha, \beta \in \mathbb{Z}$, has integer coefficients. Indeed, applying Theorem 1.1, the condition (1) with $p = 2$, $r = 1$ becomes

$$1 + \alpha x + \beta x^2 \equiv (1 + \beta x)^2 \pmod{4},$$

which is equivalent to $\alpha \equiv 2\beta$ and $\beta \equiv \beta^2 \pmod 4$. In other words, $\alpha \equiv 2\beta$ and $\beta \equiv 0, 1 \pmod 4$. Since α is necessarily even, we may set $b = -\alpha/2 \in \mathbb{Z}$ and $d = \beta$ to match the right-hand side of (4). In terms of b and d, the conditions for integrality reduce to

$$b \equiv d \pmod 2, \quad d \equiv 0, 1 \pmod 4,$$

which can be combined to $d \equiv b^2 \pmod 4$. In particular, letting $a = 1$ and $c = (b^2 - d)/4 \in \mathbb{Z}$, we conclude that, if the coefficients of $(1 + \alpha x + \beta x^2)^{-1/2}$ are integers, then they are given by the generalized trinomial coefficients $T_n(a, b, c)$.

Example 1.8. As another application of Theorem 1.1, let us characterize the values $a, b \in \mathbb{Z}$ and $\lambda \in \mathbb{Q}$, for which the power series $(1 + ax + bx^2)^\lambda$ has integer coefficients. As in Example 1.4, it follows from Theorem 1.1 that, if $p^r \neq 2$, then $(1+ax+bx^2)^{1/p^r} \in \mathbb{Z}_p[[x]]$ if and only if $a, b \in p^{r+1}\mathbb{Z}_p$. On the other hand, as in the previous example, $(1+ax+bx^2)^{1/2} \in \mathbb{Z}_2[[x]]$ if and only if either $a, b \in 4\mathbb{Z}_2$ or $(a, b) \equiv (2, 1) \pmod 4$. Let k be the denominator of λ. It follows that $(1 + ax + bx^2)^\lambda \in \mathbb{Z}[[x]]$ if and only if

- $a, b \in k \operatorname{rad}(k)\mathbb{Z}$, or
- $k = 2\kappa$ and $a, b \in \kappa \operatorname{rad}(\kappa)\mathbb{Z}$ as well as $(a, b) \equiv (2, 1) \pmod 4$.

Note that, in the second case, κ is necessarily odd.

The remainder of this paper is organized as follows. Before proving Theorem 1.1 in Section 3, we collect some basic notations and results in Section 2. In the final Section 4, we then review (and slightly extend) the Dieudonné–Dwork criterion for the purpose of comparison with Theorem 1.1.

2 Notations and review

For any formal power series $f(x) \in 1 + xR[[x]]$ over a commutative ring R containing $\mathbb{Q}$, the power $f(x)^\lambda$ can be defined for any $\lambda \in R$ as a formal power series by the binomial expansion

$$(1 + a_1x + a_2x^2 + \ldots)^\lambda = \sum_{n \geq 0} \binom{\lambda}{n} (a_1x + a_2x^2 + \ldots)^n \in R[[x]], \tag{5}$$

where

$$\binom{\lambda}{n} = \frac{\lambda(\lambda - 1) \cdots (\lambda - n + 1)}{n!}. \tag{6}$$

We refer to [KP11] and [Sam23] for introductions to formal power series. We note that the binomial expansion (5) for $(1+x)^\lambda$ is equivalent to the definition $(1+x)^\lambda = \exp(\lambda \log(1+x))$ used in [Sam23] to which we refer the reader for a detailed discussion of the formal power series $\exp(x), \log(1 + x) \in \mathbb{Q}[[x]]$ and their properties. In particular, the expansion (5) agrees with products of power series in the case where $\lambda \in \mathbb{Z}_{\geq 0}$, and the usual power laws hold. For instance, as pointed out in [KP11, §5.1], the multiplication law $f(x)^\lambda f(x)^\mu = f(x)^{\lambda+\mu}$ is equivalent to the Vandermonde convolution identity. Similarly, for any $\lambda,\mu \in R$ and $f(x) \in 1 + xR[[x]]$, we have $(f(x)^\lambda)^\mu = f(x)^{\lambda\mu}$, which can be deduced from the corresponding property $\exp(x)^\lambda = \exp(\lambda x)$ of the exponential. Note that this implies the following observation: if $f(x) = g(x)^\lambda$ for $f(x), g(x) \in 1 + xR[[x]]$ and $\lambda \in R^\times$, then we necessarily have $g(x) = f(x)^{1/\lambda}$.

For our purposes, we note that, if $\lambda \in \mathbb{Z}_p$, then $\binom{\lambda}{n} \in \mathbb{Z}_p$ for any integer $n \geq 0$ (this is clear for $\lambda \in \mathbb{Z}_{\geq 0}$ and follows for $\lambda \in \mathbb{Z}_p$ by p-adic continuity and the fact that $\mathbb{Z}_p$ is closed). Consequently, if $f(x) \in \mathbb{Z}_p[[x]]$ and $\lambda \in \mathbb{Z}_p$, then $f(x)^\lambda \in \mathbb{Z}_p[[x]]$. In particular, if $\lambda \in \mathbb{Z}_p^\times$, then $f(x) \in \mathbb{Z}_p[[x]]$ if and only if $f(x)^\lambda \in \mathbb{Z}_p[[x]]$.

Finally, we recall the following rather well-known result concerning congruences involving power series (see, for instance, [RY15, Proposition 1.9]).

Lemma 2.1. *For any $f(x), g(x) \in \mathbb{Z}_p[[x]]$ and $r \in \mathbb{Z}_{>0}$,*

$$f(x) \equiv g(x) \pmod{p} \quad\Longleftrightarrow\quad f(x)^{p^{r-1}} \equiv g(x)^{p^{r-1}} \pmod{p^r}.$$

Proof. By Fermat's little theorem for power series (which follows from the binomial expansion (5) combined with the fact that $\binom{p}{n}$ is divisible by p except if $n = 0$ or $n = p$), we have

$$f(x)^p \equiv f(x^p) \pmod{p}, \tag{7}$$

and thus $f(x)^{p^{r-1}} \equiv f(x^{p^{r-1}})$ modulo p, for any $f(x) \in \mathbb{Z}_p[[x]]$. Therefore, if $f(x)^{p^{r-1}} \equiv g(x)^{p^{r-1}}$ modulo p^r, then $f(x) \equiv g(x)$ modulo p.

For the converse, suppose that $f(x) \equiv g(x)$ modulo p. We will prove $f(x)^{p^{r-1}} \equiv g(x)^{p^{r-1}}$ modulo p^r by induction on r. For $r = 1$, this is true by assumption. Suppose that $f(x)^{p^{r-1}} \equiv g(x)^{p^{r-1}}$ modulo p^r for some $r \geq 1$. Then $f(x)^{p^{r-1}} = g(x)^{p^{r-1}} + p^r h(x)$ for some $h(x) \in \mathbb{Z}_p[[x]]$. Raising both sides to the pth power, we find

$$f(x)^{p^r} = (g(x)^{p^{r-1}} + p^r h(x))^p = g(x)^{p^r} + \sum_{k=1}^{p} \binom{p}{k} g(x)^{p^{r-1}(p-k)} (p^r h(x))^k.$$

For each $k \in \{1, 2, \ldots, p\}$, the summand on the right-hand side is divisible by at least p^{r+1}, so that we conclude $f(x)^{p^r} \equiv g(x)^{p^r}$ modulo p^{r+1}, as needed for the induction step. □

3 Proof of Theorem 1.1

In preparation for proving Theorem 1.1, we observe the following result, which can also be found, for instance, in [PS76, Part VIII, Chap. 3, No. 140]. (Note that it follows from Theorem 1.1 that, more generally, $(1 + ax)^{1/p^r} \in \mathbb{Z}_p[[x]]$ if and only if $a \in p^{r+1}\mathbb{Z}_p$.)

Lemma 3.1. *For any $r \in \mathbb{Z}_{>0}$, we have $(1 + p^{r+1}x)^{1/p^r} \in \mathbb{Z}_p[[x]]$.*

Proof. For any $n \in \mathbb{Q}_p$ (in particular, for any $n \in \mathbb{Q}$), denote with $\nu_p(n)$ the p-adic valuation of n, that is the largest $r \in \mathbb{Z}$ such that $n/p^r \in \mathbb{Z}_p$ if $n \neq 0$ (and $r = \infty$ if $n = 0$). We recall Legendre's formula which states that

$$\nu_p(n!) = \frac{n - s_p(n)}{p - 1}, \tag{8}$$

where $s_p(n)$ is the sum of the digits of n in base p. It further follows from (6) that, if $\nu_p(\lambda) < 0$, then

$$\nu_p\left(\binom{\lambda}{n}\right) = n\nu_p(\lambda) - \nu_p(n!). \tag{9}$$

In particular, by combining this with Legendre's formula, we have

$$\begin{aligned} \nu_p\left(\binom{p^{-r}}{n}\right) &= -rn - \nu_p(n!) = -\left(r + \frac{1}{p-1}\right)n + \frac{s_p(n)}{p-1} \\ &\geq -\left(r + \frac{1}{p-1}\right)n \geq -(r+1)n. \end{aligned}$$

It therefore follows that the coefficients of $(1 + ax)^{1/p^r}$ are p-integral if $\nu_p(a) \geq r + 1$. In particular, $(1 + p^{r+1}x)^{1/p^r} \in \mathbb{Z}_p[[x]]$, as claimed. $\square$

We are now in a convenient position to prove Theorem 1.1 which is restated in expanded form below. We note that the equivalence of (a) and (b) follows from the result of Heninger, Rains and Sloane [HRS06, Theorem 1] that we indicate in Example 1.6.

Theorem 3.2. *Suppose* $f(x) = 1 + a_1x + a_2x^2 + \ldots \in \mathbb{Z}_p[[x]]$ *and* $r \in \mathbb{Z}_{>0}$. *Then the following are equivalent.*

(a) $f(x)^{1/p^r} \in \mathbb{Z}_p[[x]]$

(b) $f(x) \equiv g(x)^{p^r} \pmod{p^{r+1}}$ *for some* $g(x) \in \mathbb{Z}_p[[x]]$

(c) $f(x) \equiv (1 + a_{p^r}x + a_{2p^r}x^2 + \ldots)^{p^r} \pmod{p^{r+1}}$

Proof. Note that $f(x)^{1/p^r} \in \mathbb{Z}_p[[x]]$ if and only if there exists $g(x) \in \mathbb{Z}_p[[x]]$ such that $g(x)^{p^r} = f(x)$. As such, (a) clearly implies (b).

Obviously, (c) implies (b). Let us show that the two conditions are, in fact, equivalent. To that end, suppose that (b) holds. Write $g(x) = b_0 + b_1x + b_2x^2 + \ldots$ and observe that, by repeated application of Fermat's little theorem (7),

$$g(x)^{p^r} \equiv g(x^{p^r}) = b_0 + b_1x^{p^r} + b_2x^{2p^r} + \ldots \pmod{p}.$$

Thus, it follows from $f(x) \equiv g(x)^{p^r} \pmod{p^{r+1}}$ that $b_m \equiv a_{mp^r} \pmod{p}$. In other words,

$$g(x) \equiv 1 + a_{p^r}x + a_{2p^r}x^2 + \ldots \pmod{p}.$$

By Lemma 2.1, this congruence is equivalent to

$$g(x)^{p^r} \equiv (1 + a_{p^r}x + a_{2p^r}x^2 + \ldots)^{p^r} \pmod{p^{r+1}},$$

so that condition (c) follows from (b).

Finally, suppose that condition (c) holds. We need to show that (a) holds, that is, $f(x)^{1/p^r} \in \mathbb{Z}_p[[x]]$. Write $g(x) = 1+a_{p^r}x+a_{2p^r}x^2+\ldots$, and let $\Delta(x) = f(x)-g(x)^{p^r}$. By (c), we have $\Delta(x) \in p^{r+1}x\mathbb{Z}_p[[x]]$. Observe that it follows from Lemma 3.1 that $(1+p^{r+1}x)^{1/p^r} \in \mathbb{Z}_p[[x]]$. In particular, $(1 + h(x))^{1/p^r} \in \mathbb{Z}_p[[x]]$ whenever $h(x) \in p^{r+1}x\mathbb{Z}_p[[x]]$. We therefore conclude that

$$f(x)^{1/p^r} = (g(x)^{p^r} + \Delta(x))^{1/p^r} = g(x)\left(1 + \frac{\Delta(x)}{g(x)^{p^r}}\right)^{1/p^r} \in \mathbb{Z}_p[[x]]$$

because $g(x)$, and thus $g(x)^{-p^r}$ as well, are in $1 + x\mathbb{Z}_p[[x]]$. □

4 The Dieudonné–Dwork criterion

For comparison with Theorem 1.1, we discuss in this section a well-known general criterion due to Dieudonné and Dwork that is recorded as Theorem 4.1 below. We include a proof of this criterion since we have not seen condition (c) stated in the literature (such as [Dwo58], [Lan80], [Kob84] and [Rob00]). On the other hand, Dwork's proof for the equivalence of (a) and (b) readily extends to show that (a) and (c) are equivalent as well. As mentioned in [Kob84] and [Rob00], the Dieudonné–Dwork criterion can be interpreted as saying that a power series $f(x)$ has p-integral coefficients if and only if it "commutes to within mod p" with the pth power map. Both (b) and (c) are natural ways to make such a statement precise. (We note that, given (a), the conditions (b) and (c) are clearly equivalent. However, it is not obvious to us that the conditions (b) and (c) should be equivalent without using (a) to pass from one to the other.)

Theorem 4.1 (Dieudonné–Dwork)**.** *Let $f(x) \in 1 + x\mathbb{Q}_p[[x]]$. Then the following are equivalent:*

(a) $f(x) \in \mathbb{Z}_p[[x]]$

(b) $\dfrac{f(x)^p}{f(x^p)} \equiv 1 \pmod{p}$

(c) $f(x)^p \equiv f(x^p) \pmod{p}$

Proof. We follow the proof in [Rob00, Chapter 7.2.3]. First, we show that (a) implies both (b) and (c). Suppose that $f(x) \in \mathbb{Z}_p[[x]]$. Then, by Fermat's little theorem (7), we have $f(x)^p \equiv f(x^p) \pmod{p}$ which is equivalent to $f(x)^p/f(x^p) \equiv 1$ since $f(x^p) \in 1 + \mathbb{Z}_p[[x]]$ is invertible in $\mathbb{Z}_p[[x]]$.

On the other hand, suppose that either (b) or (c) holds, and write $f(x) = 1 + a_1x + a_2x^2 + \ldots \in \mathbb{Q}_p[[x]]$. In that case, there exists $g(x) = b_1x + b_2x^2 + \ldots \in \mathbb{Z}_p[[x]]$ such that

$$f(x)^p = f(x^p) + p\varphi(x)g(x), \tag{10}$$

where $\varphi(x) = f(x^p)$ in the case of (b) and $\varphi(x) = 1$ in the case of (c). It follows that $a_1 = b_1 \in \mathbb{Z}_p$. Suppose that $a_j \in \mathbb{Z}_p$ for all $j < n$. We claim that $a_n \in \mathbb{Z}_p$ so that (a) follows by induction. To show this claim, we compare the coefficient of x^n on both sides of (10). For the left-hand side, we find

$$\begin{aligned} [x^n]f(x)^p &= [x^n](1 + a_1x + \ldots + a_nx^n)^p \\ &= pa_n + [x^n](1 + a_1x + \ldots + a_{n-1}x^{n-1})^p \\ &\equiv pa_n + [x^n](1 + a_1x^p + \ldots + a_{n-1}x^{(n-1)p}) \pmod p \\ &= pa_n + a_{n/p}. \end{aligned} \tag{11}$$

In the final step, we use the convention that $a_{n/p} = 0$ if p does not divide n. Note that we were able to use Fermat's little theorem (7) to reduce $(1 + a_1x + \ldots + a_{n-1}x^{n-1})^p$ since, by the induction hypothesis, all coefficients are in $\mathbb{Z}_p$. On the other hand, for the right-hand side of (10), the only coefficients of $f(x^p)$ and $\varphi(x)$ contributing to the coefficient of x^n are in $\mathbb{Z}_p$. Further reducing modulo p, only $f(x^p)$ contributes, whose coefficient of x^n is $a_{n/p}$. Upon comparison with (11), we conclude that $pa_n \in p\mathbb{Z}_p$ or, equivalently, $a_n \in \mathbb{Z}_p$, as claimed. □

Theorem 1.1 was proved by Dwork [Dwo58] who credits Dieudonné [Die57] for proving the following additive version (both consider the special case where $f(x)$ has the form $\sum_{n\geq 0} a_nx^{p^n}$). Since both results are often referred to as Dwork's lemma in the literature, we find it fitting to include this additive version here, highlighting that it is consequence of Theorem 4.1.

Corollary 4.2 (Dieudonné–Dwork, additive version)**.** *Let* $f(x) \in x\mathbb{Q}_p[[x]]$*. Then* $\exp(f(x)) \in \mathbb{Z}_p[[x]]$ *if and only if* $f(x^p) - pf(x) \in p\mathbb{Z}_p[[x]]$*.*

Proof. It follows from Theorem 4.1 that $\exp(f(x)) \in \mathbb{Z}_p[[x]]$ if and only if

$$\exp(f(x^p) - pf(x)) \equiv 1 \pmod{p\mathbb{Z}_p[[x]]}.$$

The claim therefore follows from

$$\exp\left(\sum_{n\geq 1} a_nx^n\right) \in p\mathbb{Z}_p[[x]] \quad\Longleftrightarrow\quad \sum_{n\geq 1} a_nx^n \in p\mathbb{Z}_p[[x]]. \tag{12}$$

The "$\Longleftarrow$" part of this equivalence is a consequence of the fact that $\exp(px) \in 1 + px\mathbb{Z}_p[[x]]$ (see, for instance, [Rob00, Chapter 7.2.3]). On the other hand, suppose that the left-hand side of (12) holds but that the right-hand side does not. In that case, there exists $N \geq 1$ such that $a_N \notin p\mathbb{Z}_p$. Suppose that N is chosen as small as possible. Since $\exp\left(\sum_{n<N} a_n x^n\right)$ as well as its inverse are in $1 + px\mathbb{Z}_p[[x]]$, we conclude that $\exp\left(\sum_{n\geq N} a_n x^n\right) \in p\mathbb{Z}_p[[x]]$. The coefficient of x^N in that series is a_N so that, in particular, $a_N \in p\mathbb{Z}_p$. This, however, is a contradiction. □

There are various directions in which Theorem 4.1 and Corollary 4.2 can be extended, including to several variables and extensions of $\mathbb{Q}_p$. We refer the interested reader to [Rob00] for more information. For recent work on truncated versions of this integrality criterion, we refer to [KM15]. Here, for comparison with Theorem 1.1, we offer the following slight extension of the Dieudonné–Dwork criterion as stated in Theorem 4.1 (which is the case $r = 0$ of the following).

Corollary 4.3. *Let $f(x) \in 1 + x\mathbb{Q}_p[[x]]$ and $r \in \mathbb{Z}_{\geq 0}$. Then the following are equivalent:*

(a) $f(x)^{1/p^r} \in \mathbb{Z}_p[[x]]$

(b) $\dfrac{f(x)^p}{f(x^p)} \equiv 1 \pmod{p^{r+1}}$

(c) $f(x)^p \equiv f(x^p) \pmod{p^{r+1}}$

Proof. It follows from Theorem 4.1 that conditions (b) and (c) imply $f(x) \in \mathbb{Z}_p[[x]]$. Since condition (a) clearly implies $f(x) \in \mathbb{Z}_p[[x]]$ as well, we may assume throughout that $f(x) \in 1+x\mathbb{Z}_p[[x]]$. This assumption, in particular, implies that $1/f(x) \in \mathbb{Z}_p[[x]]$ so that it becomes clear that conditions (b) and (c) are equivalent.

Recall from Lemma 2.1 that, for p-integral power series, $f(x)^{p^r} \equiv g(x)^{p^r} \pmod{p^{r+1}}$ is equivalent to $f(x) \equiv g(x) \pmod{p}$. Consequently, condition (b) is equivalent to

$$\left(\frac{f(x)^p}{f(x^p)}\right)^{1/p^r} \equiv 1 \pmod{p}.$$

By the Dieudonné–Dwork criterion as in Theorem 4.1, applied with $f(x)^{1/p^r}$ in place of $f(x)$, it follows that this latter congruence is equivalent to $f(x)^{1/p^r} \in \mathbb{Z}_p[[x]]$, which is condition (a). □

In [Rob00], the Dieudonné–Dwork criterion is described by stating that "the extent to which the operations

- first raising x to the power p and then applying f,
- first computing $f(x)$ and then raising to the pth power

lead to similar results, is a measure of the integrality of the coefficients of $f(x)$." Corollary 4.3 can be interpreted as a quantifiable version of this statement. Corollary 4.3 also provides a second characterization of the p-integrality of power series $f(x)^{1/p^r}$ which differs from the characterization we offer in Theorem 1.1. To appreciate this difference, we conclude with the following example.

Example 4.4. As observed in Example 1.4, Theorem 1.1 immediately implies that, if $a_1, a_2, \ldots, a_d \in \mathbb{Z}_p$ with $d < p^r$, then $(1 + a_1x + a_2x^2 + \ldots + a_dx^d)^{1/p^r} \in \mathbb{Z}_p[[x]]$ if and only if $a_1, a_2, \ldots, a_d \in p^{r+1}\mathbb{Z}_p$. On the other hand, applying Corollary 4.3 to this case, we find that $(1 + a_1x + a_2x^2 + \ldots + a_dx^d)^{1/p^r} \in \mathbb{Z}_p[[x]]$ if and only if

$$(1 + a_1x + a_2x^2 + \ldots + a_dx^d)^p \equiv 1 + a_1x^p + a_2x^{2p} + \ldots + a_dx^{pd} \pmod{p^{r+1}}.$$

It then requires additional thought to conclude that this congruence is equivalent to $a_1, a_2, \ldots, a_d \in p^{r+1}\mathbb{Z}_p$.

Acknowledgements

We thank Tewodros Amdeberhan and Christoph Koutschan for valuable comments on earlier drafts of this paper. We are also grateful to the referee for helpful comments that made the paper more focused, as well as for suggesting the present proof of Corollary 4.3 that avoids use of Theorem 1.1.

The second author gratefully acknowledges support through a Collaboration Grant (#514645) awarded by the Simons Foundation.

References

[Die57] Jean Dieudonné. On the Artin-Hasse exponential series. *Proceedings of the American Mathematical Society*, 8(2):210–214, 1957.

[Dwo58] Bernard M. Dwork. Norm residue symbol in local number fields. *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, 22(1):180–190, 1958.

[HRS06] Nadia Heninger, Eric M. Rains, and Neil J. A. Sloane. On the integrality of nth roots of generating functions. *Journal of Combinatorial Theory, Series A*, 113(8):1732–1745, 2006.

[KM15] Christian Krattenthaler and Thomas W. Müller. Truncated versions of Dwork's lemma for exponentials of power series and p-divisibility of arithmetic functions. *Advances in Mathematics*, 283:489–529, 2015.

[Kob84] Neal Koblitz. *p-adic Numbers, p-adic Analysis, and Zeta Functions*. Springer, New York, 2nd edition, 1984.

[KP11] Manuel Kauers and Peter Paule. *The Concrete Tetrahedron.* Springer-Verlag, 2011.

[Lan80] Serge Lang. *Cyclotomic Fields II.* Springer-Verlag, New York, 1980.

[Noe06] Tony D. Noe. On the divisibility of generalized central trinomial coefficients. *Journal of Integer Sequences*, 9(2):06.2.7, 2006.

[PS76] George Pólya and Gabor Szegö. *Problems and Theorems in Analysis*, volume II. Springer, 1976.

[Rob00] Alain M. Robert. *A Course in p-adic Analysis.* Springer, New York, 2000.

[RY15] Eric Rowland and Reem Yassawi. Automatic congruences for diagonals of rational functions. *Journal de Théorie des Nombres de Bordeaux*, 27(1):245–288, 2015.

[Sam23] Benjamin Sambale. An Invitation to Formal Power Series. *Jahresbericht der Deutschen Mathematiker-Vereinigung*, 125:3–69, 2023.

[SMA09] Armin Straub, Victor H. Moll, and Tewodros Amdeberhan. The p-adic valuation of k-central binomial coefficients. *Acta Arithmetica*, 140(1):31–42, 2009.