On the characterization of base-*p* number representations

Summary: We treat number representations with natural bases $p>1$. For this, we show that for prime bases p the digits of the representation $a_m a_{m-1}\dots a_n\dots a_1 a_0$ of a given number z can be characterized by means of certain binomial coefficients. The main result is as follows: provided a_n is the n-th digit of the base-*p* representation of z then the congruency $\binom{z}{p^n} \equiv a_n \pmod p$ holds true. In addition, this statement is proved to be false in the general case of non-prime bases.

Zusammenfassung: Wir betrachten polyadische Zahldarstellungen mit natürlichen Basen $p>1$ und zeigen, dass für Primzahlbasen p die entsprechenden Ziffern $a_m a_{m-1}\dots a_n\dots a_1 a_0$ mittels bestimmter Binomialkoeffizienten charakterisiert werden können. Für die *n*-te Ziffer a_n in der Darstellung von z zur Basis p besteht die Kongruenz $\binom{z}{p^n} \equiv \left\lfloor \frac{z}{p^n} \right\rfloor \equiv a_n \pmod p$. Für Nichtprimzahlbasen trifft dies im Allgemeinen nicht zu.

By Hieronymus Fischer

1. Introduction

We discuss base-*p* number representations $z := a_m a_{m-1}\dots a_n\dots a_1 a_0$ with natural bases $p>1$. In polynomial notation the unique representation is $z=\sum_{\mu=0}^{m} a_\mu p^\mu$, $0\le a_\mu < p$. For a given non-negative number z the parameters a_μ can be determined by means of a simple algorithm. This follows from the polynomial representation since the integer part of $\frac{z}{p^n}$ is $a_n + \sum_{\mu=n+1}^{m} a_\mu p^{\mu-n}$ and so $a_n \equiv \left\lfloor \frac{z}{p^n} \right\rfloor \pmod p$ for $0\le n\le m$. In the following we will demonstrate that for prime bases *p* the parameters, or rather the digits a_n fulfill a quite similar congruency in terms of binomial coefficients.

We provide the main result for arbitrary prime bases in section 3. An alternative approach, which results in a weaker statement, will be discussed in section 2. There we highlight the case *p=2*, especially.

We start with some definitions.

Definition 1-1

For natural numbers $n, z \geq 0$ *we use the notation* $a_n^{[z]}$ *to indicate the n-th coefficient of the base-p representation of* z. *Explicitly* $a_n^{[z]} := a_n$ *if* $z = \sum_{\mu=0}^{m} a_\mu p^\mu,\ 0 \leq a_\mu < p,\ \ 0 \leq n \leq m$ *and* $a_n^{[z]} := 0$ *for* $n > m$.

Definition 1-2

Following the Kronecker symbol we define $\delta(x, y) := \begin{cases} 1, & x = y \\ 0, & \text{else} \end{cases}$

Definition 1-3

For non-negative numbers z represented as $z = \sum_{\mu=0}^{m} a_\mu p^\mu,\ 0 \leq a_\mu < p,$ *p prime, we set* $\Delta_{nk}(z) := \prod_{\mu=n}^{k-1} \delta(0, a_\mu)$, *with* $n, k \in \mathbb{N}_0,\ \ 0 \leq n, k \leq m$.

2. Number representation versa prime divisors of certain binomial coefficients

We ask for the highest power of a prime p dividing the binomial coefficient $\binom{z}{p^n}$. For the general case of $\binom{m+k}{k}$ this has been discussed by Kummer first. Essentially, the findings presented in this section can also be derived from Kummer's results. However, our goal is to get predicates on the radix-p representation and so a different approach seems to be more appropriate. The following lemma provides an exhaustive answer to the posed question in terms of the base-p representation of z. As an application we prove an obvious corollary for representations of z with prime radixes. Especially we will characterize the representation of binary numbers (s. Theorem 2-2).

Lemma 2-1

Let n and z be natural numbers, and let p *be a prime. Suppose that* $\sum_{\mu=0}^{m} a_\mu p^\mu,\ 0 \leq a_\mu < p$, *is the base-p representation of z.*

Then $q := p^r$, *where* $r := \sum_{k=n+1}^{m} \Delta_{nk}(z)$ *, is the highest power of* p *dividing* $\binom{z}{p^n}$

Proof:

For natural x we set

(2-1) $$E_p(x) := \max\left\{ t \in \mathbb{N}_0 \mid p^t \mid x \right\}$$

and

(2-2) $$F_p(x) := \max\left\{ t \in \mathbb{N}_0 \mid p^t \mid x! \right\}$$

By definition of the factorial, $x! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot \ldots \cdot (x-1) \cdot x$, we see, that the multiples of p arise $\left\lfloor \frac{x}{p} \right\rfloor$-times in this product whereas the multiples of p^2 occur $\left\lfloor \frac{x}{p^2} \right\rfloor$-times. In general, the multiples of a given power p^k appear exactly $\left\lfloor \frac{x}{p^k} \right\rfloor$ times as a factor in $x!$. For that reason, the exponent of the highest power of x dividing $x!$ is determined by the sum of all such terms with $p^k \le x$, what means $k \le \log_p x$. Hence

(2-3) $$F_p(x) = \sum_{k=1}^{\lfloor \log_p x \rfloor} \left\lfloor \frac{x}{p^k} \right\rfloor$$

Based on this we are able to determine the highest power of p dividing $\binom{z}{p^n}$ by simply evaluating the exponent $r := E_p\left(\binom{z}{p^n}\right)$ with respect to $\binom{z}{p^n} = \frac{z!}{p^n!\left(z-p^n\right)!}$. Obviously, we have

(2-4) $$r = F_p(z) - F_p(p^n) - F_p(z-p^n)$$

By definition of z we get $m = \lfloor \log_p z \rfloor$. Further we set $m' := \lfloor \log_p (z-p^n) \rfloor$.
It follows

(2-5) $$F_p(z) = \sum_{k=1}^{m} \left\lfloor \frac{z}{p^k} \right\rfloor$$

$$F_p(p^n) = \sum_{k=1}^{m} \left\lfloor \frac{p^n}{p^k} \right\rfloor$$

(2-6) $$= \sum_{k=1}^{n} p^{n-k}$$

$$= \frac{p^n - 1}{p-1}$$

$$F_p(z-p^n) = \sum_{k=1}^{m'} \left\lfloor \frac{z-p^n}{p^k} \right\rfloor$$

(2-7) $$= \sum_{k=1}^{m'} \left\lfloor \frac{z}{p^k} - p^{n-k} \right\rfloor$$

$$= \sum_{k=1}^{n} \left\lfloor \frac{z}{p^k} \right\rfloor - \frac{p^n - 1}{p-1} + \sum_{k=n+1}^{m'} \left\lfloor \frac{z-p^n}{p^k} \right\rfloor$$

For the exponent we subsequently obtain by (2-4)

(2-8) $$r = \sum_{k=n+1}^{m} \left\lfloor \frac{z}{p^k} \right\rfloor - \sum_{k=n+1}^{m'} \left\lfloor \frac{z-p^n}{p^k} \right\rfloor$$

Now, for $n < m$ the equality $m' = m$ is evident by definition of m and m'. On the other hand, if $m' < m$ then stringently $n = m$, from which follows $r = 0$, since both sums in (2-8) evaluates to zero in this case. In the following we may restrict ourselves to $n < m$ and thus $m' = m$.

To come to (2-8) we first get

(2-9) $$\left\lfloor \frac{z}{p^k} \right\rfloor = \sum_{\mu=k}^{m} a_\mu p^{\mu-k}$$

and

(2-10) $$\frac{z-p^n}{p^k} = \sum_{\mu=k}^{m} a_\mu p^{\mu-k} + \sum_{\mu=1}^{k-1} a_\mu p^{\mu-k} - p^{n-k}$$

The second sum in (2-10) is non-negative and less than one. Hence, for $k \le n$, the integer part yields

(2-11) $$\left\lfloor \frac{z-p^n}{p^k} \right\rfloor = \sum_{\mu=k}^{m} a_\mu p^{\mu-k} - p^{n-k}$$

With the definition

(2-12) $$D_{nk} := \sum_{\mu=1}^{k-1} a_\mu p^{\mu-k} - p^{n-k}$$

it follows for $k > n$

(2-13) $$\left\lfloor \frac{z-p^n}{p^k} \right\rfloor = \sum_{\mu=k}^{m} a_\mu p^{\mu-k} + \lfloor D_{nk} \rfloor$$

Now, we must distinguish whether or not the difference D_{nk} is negative. It is non-negative, if there is an index $\mu,\ n \le \mu < k$, such that $a_\mu > 0$. The difference becomes negative, iff $a_\mu = 0$ for all $\mu,\ n \le \mu < k$. The absolute values always are less then 1. Therefore, we get

(2-14) $$\lfloor D_{nk} \rfloor = \begin{cases} -1, & \forall \mu \in IN, n \le \mu < k : a_\mu = 0 \\ 0, & \text{else} \end{cases}$$

Together with (2-8), (2-9) and (2-13) this results in

$$
\begin{aligned}
r &= \sum_{k=n+1}^{m} \left\lfloor \frac{z}{p^k} \right\rfloor - \sum_{k=n+1}^{m} \left\lfloor \frac{z-p^n}{p^k} \right\rfloor \\
&= \sum_{k=n+1}^{m} \sum_{\mu=k}^{m} a_\mu p^{\mu-k} - \sum_{k=n+1}^{m} \left(\sum_{\mu=k}^{m} a_\mu p^{\mu-k} + \lfloor D_{nk} \rfloor \right) \\
&= -\sum_{k=n+1}^{m} \lfloor D_{nk} \rfloor
\end{aligned}
\tag{2-15}
$$

Because of (2-14) we may replace $\lfloor D_{nk} \rfloor = -\prod_{\mu=n}^{k-1} \delta(0, a_\mu) = -\Delta_{nk}(z)$ from which follows

$$
r = \sum_{k=n+1}^{m} \Delta_{nk}(z) \tag{2-16}
$$

This is also true for the case $n = m$. Thus $p^r = \prod_{k=n+1}^{m} p^{\Delta_{nk}(z)}$ is the highest $\binom{z}{p^n}$ dividing power of p. □

For binary numbers the exponent r of the highest power of 2 dividing $\binom{z}{2^n}$ can be evaluated very easily. Provided z is given by $z := \sum_{\mu=0}^{m} a_\mu 2^\mu$, $a_\mu \in \{0,1\}$, then the lemma above yields $r := \sum_{k=n+1}^{m} \prod_{\mu=n}^{k-1} (1 - a_\mu)$. With respect to Definition 1-2 and Definition 1-3 this is an immediate result of Lemma 2-1 because of $a_\mu \in \{0,1\}$, and therefore $\delta(0, a_n) = 1 - a_n$.

Theorem 2-1

Let z be a natural number, and let p be a prime. Suppose $\sum_{\mu=0}^{m} a_\mu p^\mu$, $0 \le a_\mu < p$, is the base-p representation of z.

Then, for all n, $0 \le n \le m$: $\binom{z}{p^n} \equiv 0 \pmod{p}$ if and only if $a_n = 0$.

Proof:

We have to demonstrate: p divides $\binom{z}{p^n} \Leftrightarrow a_n = 0$.

For $z = p^n$ we have $\binom{z}{p^n} = 1$ and so $a_n = 1 \neq 0$ in accordance with the statement. In the following we may presume $z > p^n$ therefore. Due to Lemma 2-1, the exponent of the highest power of p dividing $\binom{z}{p^n}$ is determined by $r := \sum_{k=n+1}^{m} \Delta_{nk}(z) = \sum_{k=n+1}^{m} \prod_{\mu=n}^{k-1} \delta(0, a_\mu)$.

Obviously, $r > 0$ is equivalent with $\binom{z}{p^n} = 0 \pmod p$. Thus we are ready, if we can verify $r = 0 \Leftrightarrow a_n > 0$.

For $a_n > 0$ we also have $\delta(0, a_n) = 0$. Consequently all products $\prod_{\mu=n}^{k-1} \delta(0, a_\mu)$, $n < k \le m$, evaluates to zero, hence $r = 0$. On the other hand, the latter forces $\prod_{\mu=n}^{k-1} \delta(0, a_\mu) = 0$ for all k, $n < k \le m$. In particularly this means $\delta(0, a_n) = 0$, Therefore $a_n \neq 0$, i.e. $a_n > 0$, respectively.

The equivalence $r = 0 \Leftrightarrow a_n > 0$ is verified therewith. □

Theorem 2-2

Let z be a natural number with $z := \sum_{\mu=0}^{m} a_\mu 2^\mu$, $a_\mu \in \{0,1\}$, *as the binary representation of z.*

Then, for all $n, 0 \le n \le m$, *the congruency* $a_n \equiv \binom{z}{2^n} \pmod 2$ *holds true.*

Proof:

By reason of Theorem 2-1 we have $\binom{z}{2^n} \equiv 0 \pmod 2 \Leftrightarrow a_n = 0$. Since the values a_n are either 0 or 1, the proposition is verified. □

3. The characterization of number representations of prime radix

In this section we prove the main result on the characterization of number representations of prime radix (s. Theorem 3-1).

First of all we recall some useful basics concerning the residue calculus in $\mathbb{Z}_p$. Most important: for prime numbers p $\mathbb{Z}_p$ is a field. The element $p-1 \equiv -1 \pmod p$ is self-invers. Due to the fact that all the residues $2, 3, \ldots, (p-2)$ have unique inverses unlike 1 and $p-1$, the factorial congruency

(3-1) $$(p-1)! \equiv -1 \pmod p$$

plainly holds true. With the commonly used convention $(n)_k := n(n-1)(n-2)\cdot\ldots\cdot(n-k+1)$ we have

(3-2) $$\frac{(n)_p}{p} \equiv -\left\lfloor \frac{n}{p} \right\rfloor \pmod{p}$$

since any residue $1, 2, 3, \ldots, (p-1)$ modulo p arises exactly once in the product $(n)_p$ (for $n \geq p$) and accurately one of these values is divisible by p. For $n < p$ both sides vanishes anyway. Thus, the 'size' of the left hand side quotient is given by the integer part of the fraction $\frac{n}{p}$. If we consider multiples of p in particular, we obtain subsequently

(3-3) $$\frac{(np)_p}{p} \equiv -n \pmod{p}$$

By reason of $(n)_k = \binom{n}{k} k!$ we may write the latter as $\binom{np}{p}(p-1)! \equiv -n \pmod{p}$ what leads to the congruency

(3-4) $$\binom{np}{p} \equiv n \pmod{p}$$

immediately. The following representation for the factorial of a product is useful sometimes.

(3-5) $$(m \cdot n)! = \prod_{\nu=1}^{m} (\nu n)_n$$

This formula is an outcome of the following consideration:

(3-6)
$$\begin{aligned}
(m \cdot n)! &= mn(mn-1)(mn-2) \cdot \ldots \cdot (mn-n+1) \cdot \\
&\quad \cdot ((m-1)n)((m-1)n-1)((m-1)n-2) \cdot \ldots \cdot ((m-1)n-n+1) \cdot \\
&\quad \cdot ((m-2)n)((m-2)n-1)((m-2)n-2) \cdot \ldots \cdot ((m-2)n-n+1) \cdot \\
&\quad \vdots \\
&\quad \cdot (2n)(2n-1)(2n-2) \cdot \ldots \cdot (2n-n+1) \cdot \\
&\quad \cdot n(n-1)(n-2) \cdot \ldots \cdot (n-n+1) \\
&= (mn)_n ((m-1)n)_n ((m-2)n)_n \cdot \ldots \cdot (2n)_n (1n)_n \\
&= \prod_{\nu=1}^{m} (\nu n)_n
\end{aligned}$$

Of course, we may notate this in terms of binomial coefficients too:

(3-7) $$(m\cdot n)!=(n!)^m\prod_{\nu=1}^{m}\binom{\nu n}{n}$$

By the way: if we transpose the roles of m and n, the symmetry of that formula becomes self-evident. In that case we obtain $\prod_{\mu=1}^{m}(\mu n)_n=(m\cdot n)!=\prod_{\nu=1}^{n}(m\nu)_m$.

When dividing the products of appropriate factorials, we get a concise result, as follows from the preceding.

(3-8) $$\frac{(m\cdot n)!}{(k\cdot n)!}=\prod_{\nu=k+1}^{m}(\nu n)_n,\ m\geq k$$

The deduction principle presented in the next formula is most important for the following.

(3-9) $$\begin{aligned}\frac{(k+mn)!}{k!}&=\prod_{\nu=k+1}^{k+mn}\nu\\&=\prod_{\nu=1}^{mn}(k+\nu)\\&=\prod_{\nu=1}^{m}(k+\nu n)_n\end{aligned}$$

This can be verified analogous to (3-6). With respect to the determination of definite congruences modulo p this factorial relations are helpful when used in connection with (3-3). For example, we achieve

(3-10) $$\begin{aligned}\frac{(mp)!}{m!\,p^m}&=\frac{1}{m!\,p^m}\prod_{\nu=1}^{m}(\nu p)_p\\&=\frac{1}{m!}\prod_{\nu=1}^{m}\frac{(\nu p)_p}{p}\\&\equiv\frac{1}{m!}\prod_{\nu=1}^{m}(-\nu)\\&\equiv(-1)^m\pmod p\end{aligned}$$

The binomial coefficients relevant in this section, can be treated analytically than. In doing so, from (3-5) (setting $m=p^{n-1}$ and $n=p$) we get

(3-11) $$p^n!=\left(p^{n-1}\cdot p\right)!=\prod_{\nu=1}^{p^{n-1}}(\nu p)_p=(p!)^{p^{n-1}}\prod_{\nu=1}^{p^{n-1}}\binom{\nu p}{p}$$

Further

(3-12) $$\left(mp^{n+1}\right)! = \left(mp^n \cdot p\right)! = \prod_{\nu=1}^{mp^n} \left(\nu p\right)_p = \left(p!\right)^{mp^n} \prod_{\nu=1}^{mp^n} \binom{\nu p}{p}$$

as well as

(3-13) $$\begin{aligned}\left(mp^{n+1} + p^n\right)! &= \left(\left(mp^n + p^{n-1}\right) \cdot p\right)! \\ &= \prod_{\nu=1}^{mp^n+p^{n-1}} \left(\nu p\right)_p = \left(p!\right)^{mp^n+p^{n-1}} \prod_{\nu=1}^{mp^n+p^{n-1}} \binom{\nu p}{p}\end{aligned}$$

Altogether, we obtain the relation

(3-14) $$\begin{aligned}\binom{mp^{n+1} + p^n}{p^n} &= \frac{\left(mp^{n+1} + p^n\right)!}{\left(mp^{n+1}\right)!\, p^n\,!} \\ &= \frac{\prod_{\nu=1}^{mp^n+p^{n-1}} \left(\nu p\right)_p}{\prod_{\nu=1}^{mp^n} \left(\nu p\right)_p \cdot \prod_{\nu=1}^{p^{n-1}} \left(\nu p\right)_p} \\ &= \frac{\prod_{\nu=mp^n+1}^{mp^n+p^{n-1}} \left(\nu p\right)_p}{\prod_{\nu=1}^{p^{n-1}} \left(\nu p\right)_p}\end{aligned}$$

Hence

(3-15) $$\binom{mp^{n+1} + p^n}{p^n} = \frac{\prod_{\nu=1}^{p^{n-1}} \left(mp^{n+1} + \nu p\right)_p}{\prod_{\nu=1}^{p^{n-1}} \left(\nu p\right)_p}$$

Based on this preparation we are now able to verify that statement of congruency recorded below.

Lemma 3-1

For prime numbers p and $m, n \in \mathbb{N}_0$, the following holds true

(3-16) $$\binom{mp^{n+1} + p^n}{p^n} \equiv 1 \pmod{p}$$

To prove this, we refer to (3-15) and will initially show the evidence of a further lemma by induction.

Lemma 3-2

For prime numbers p *and* $m \in \mathbb{N}_0, n \in \mathbb{N}$, *the following holds true*

$$p^{-\frac{p^n-1}{p-1}} \prod_{\nu=1}^{p^{n-1}} \left(mp^n + \nu p\right)_p \equiv (-1)^{\frac{p^n-1}{p-1}} \pmod{p} \tag{3-17}$$

Proof:

We denote the left hande side of (3-17) by $F(n)$. Setting $n=1$ we get

$$\begin{aligned} F(1) &= p^{-\frac{p-1}{p-1}} \prod_{\nu=1}^{p^0} \left(mp + \nu p\right)_p \\ &= \frac{\left(\left(mp+1\right)p\right)_p}{p} \end{aligned} \tag{3-18}$$

and so, by (3-3),

$$\begin{aligned} F(1) &\equiv -\left(mp+1\right) \\ &\equiv (-1)^{\frac{p-1}{p-1}} \pmod{p} \end{aligned} \tag{3-19}$$

For the induction step we conclude as follows:

$$\begin{aligned} F(n+1) &= p^{-\frac{p^{n+1}-1}{p-1}} \prod_{\nu=1}^{p^n} \left(mp^{n+2} + \nu p\right)_p \\ &= p^{-\frac{p^{n+1}-1}{p-1}} p^{p^n} \prod_{\nu=1}^{p^n} \frac{\left(\left(mp^{n+1} + \nu\right)p\right)_p}{p} \\ &\equiv p^{-\frac{p^{n+1}-1}{p-1}} p^{p^n} \prod_{\nu=1}^{p^n} (-1)\left(mp^{n+1} + \nu\right) \pmod{p} \end{aligned} \tag{3-20}$$

Here, the very last conversion holds true by reason of (3-3). Further we get

$$\begin{aligned} F(n+1) &\equiv p^{-\frac{p^{n+1}-1}{p-1}} p^{p^n} \prod_{\nu=1}^{p^n} (-1) \cdot \prod_{\nu=1}^{p^n} \left(mp^{n+1} + \nu\right) \\ &\equiv (-1)^{p^n} p^{-\frac{p^n-1}{p-1}} \cdot \prod_{\nu=1}^{p^n} \left(mp^{n+1} + \nu\right) \pmod{p} \end{aligned} \tag{3-21}$$

Very analogous to the deduction achieved in (3-9) we verify

$$\prod_{\nu=1}^{p^n} \left(mp^{n+1} + \nu\right) = \prod_{\nu=1}^{p^{n-1}} \left(mp^{n+1} + \nu p\right)_p \tag{3-22}$$

Thus, we subsequently obtain the congruences

$$F(n+1) \equiv (-1)^{p^n} \; p^{-\frac{p^n-1}{p-1}} \prod_{\nu=1}^{p^{n-1}} \left(mp^{n+1} + \nu p\right)_p$$

(3-23)

$$\equiv (-1)^{p^n} \cdot (-1)^{\frac{p^n-1}{p-1}}$$

$$\equiv (-1)^{\frac{p^{n+1}-1}{p-1}} \pmod{p}$$

□

Now we are able to complete the proof of Lemma 3-1:

Due to (3-15) and (3-17) we have the relation

$$\binom{mp^{n+1} + p^n}{p^n} = \frac{p^{-\frac{p^n-1}{p-1}} \cdot \prod_{\nu=1}^{p^{n-1}} \left(mp^{n+1} + \nu p\right)_p}{p^{-\frac{p^n-1}{p-1}} \cdot \prod_{\nu=1}^{p^{n-1}} (\nu p)_p}$$

(3-24)

$$\equiv \frac{(-1)^{\frac{p^n-1}{p-1}}}{(-1)^{\frac{p^n-1}{p-1}}}$$

$$\equiv 1 \pmod{p}$$

where the denominator above is determined by (3-17) when setting $m = 0$ there. □

Theorem 3-1

Let z be a natural number, and let p be a prime number. Suppose $\sum_{\mu=0}^{m} a_\mu p^\mu$, $0 \le a_\mu < p$, *is the representation of z in radix p. Then* $a_n \equiv \binom{z}{p^n} \pmod{p}$ *for* $0 \le n \le m$.

Proof:

We perform the proof by induction over the numbers *z* to be represented. The verification must be done for all n , $0 \le n \le m$. Thereby we may restrict ourselves on $n > 0$, since $\binom{z}{p^0} = z$ and $z \equiv a_0 \pmod{p}$ which implies that the statement is evidently true for *n*=0.

For a given n the induction starts with $z = p^n$. The formula is trivially true in that case. For the induction step $z \mapsto z+1$ we rest on the following relation for binomial coefficients

(3-25)

$$\binom{z+1}{p^n}\left(z+1-p^n\right) = \binom{z}{p^n}(z+1)$$

On both sides, we consider the residue classes modulo p . The corresponding values for the remainders of $\binom{z}{p^n}$ modulo p will be denoted by $a = a(n,z)$.

In general, we express $\binom{z}{p^n}$ as $\beta p + a(n,z)$ with an appropriate integer $\beta \geq 0$. By induction hypothesis $a = a(n,z) = a_n^{[z]}$ holds true. Likewise, there exists an integer $\gamma \geq 0$ and a $a = a(n,z+1) \geq 0$, such that $\gamma p + a = \binom{z+1}{p^n}$.

It is necessary to show, that $a_n^{[z+1]}$ (the *n*-th digit of the radix-*p* representation of *z*+1) equals $a = a(n,z+1)$.

In the following, we suppress the superscript index in the base-*p* representation of *z* to shorten the notation; in doing so, we write a_n instead of $a_n^{[z]}$. Explicitly we begin with

(3-26) $$z \coloneqq \sum_{\mu=0}^{m} a_\mu p^\mu,\ 0 \leq a_\mu < p$$

and define

(3-27) $$m_0 \coloneqq \begin{cases} \max\left(k \,\middle|\, \forall \mu \in \mathbb{N}, 0 \leq \mu < k : a_\mu = p-1\right), & \text{if } a_0 = p-1 \\ 0, & \text{else} \end{cases}$$

So that we get

(3-28) $$z+1 = \left(a_{m_0}+1\right)p^{m_0} + \sum_{\mu=m_0+1}^{m} a_\mu p^\mu$$

and continuing

(3-29) $$z+1-p^n = \begin{cases} \left(a_{m_0}+1\right)p^{m_0} + \sum_{\mu=m_0+1}^{n-1} a_\mu p^\mu + \sum_{\mu=n}^{m_n-1}(p-1)p^\mu + \left(a_{m_n}+1\right)p^{m_n} + \sum_{\mu=m_n+1}^{m} a_\mu p^\mu, & m_0 < n \\ \sum_{\mu=n}^{m} a_\mu p^\mu, & m_0 = n \\ \sum_{\mu=n}^{m_n-1}(p-1)p^\mu + \sum_{\mu=m_n}^{m} a_\mu p^\mu, & m_0 > n \end{cases}$$

Herein, the auxiliary integer m_n is defined by

(3-30) $$m_n \coloneqq \min\left(k \geq n \,\middle|\, a_k > 0\right)$$

Further, substituting

(3-31) $$A_k \coloneqq \sum_{\mu=k}^{m} a_\mu p^{\mu-k}$$

(3-32) $$B_k := \sum_{\mu=k}^{n-1} a_\mu p^{\mu-k} + \sum_{\mu=n}^{m_n-1} (p-1) p^{\mu-k} + \left(a_{m_n}+1\right) p^{m_n-k} + \sum_{\mu=m_n+1}^{m} a_\mu p^{\mu-k}$$

we can write (3-28) and (3-29) shorter as

(3-33) $$z+1 = \left(\left(a_{m_0}+1\right) + A_{m_0+1} p\right) p^{m_0}$$

and

(3-34) $$z+1-p^n = \begin{cases} \left(\left(a_{m_0}+1\right) + B_{m_0+1} p\right) p^{m_0}, & m_0 < n \\ \left(a_{m_0} + A_{m_0+1} p\right) p^{m_0}, & m_0 = n \\ \left(\left(p^{m_0-n}-1\right) + A_{m_0} p^{m_0-n}\right) p^n, & m_0 > n \end{cases}$$

With respect to $a_{m_0}+1 < p$ (by definition of m_0) and the primality of p we are allowed to conclude $\binom{z+1}{p^n} \equiv a_n^{[z+1]} \pmod{p}$. To understand this we resort to (3-25). There we explicitly substitute the binomial coefficients as described above. So that we obtain

(3-35) $$\left(\gamma p + a\right)\left(z+1-p^n\right) = \left(\beta p + a_n\right)\left(z+1\right)$$

For the detailed discussion we distinguish between three different cases:

(i) $m_0 < n$, by definition of m_0 we have $a_n^{[z+1]} = a_n$ then.

(ii) $m_0 = n$, by definition of m_0 we have $a_n^{[z+1]} = a_n + 1$ then.

(iii) $m_0 > n$, by definition of m_0 we have $a_n^{[z+1]} = 0$ then.

Ad (i): From (3-33) and (3-34) it follows

(3-36) $$\left(\gamma p + a\right)\left(\left(a_{m_0}+1\right) + B_{m_0+1} p\right) p^{m_0} = \left(\beta p + a_n\right)\left(\left(a_{m_0}+1\right) + A_{m_0+1} p\right) p^{m_0}$$

where $a := a\left(n, z+1\right)$. Further we get

(3-37) $$\begin{aligned} \left(a_{m_0}+1\right)\left(a-a_n\right) = {} & \left(\beta A_{m_0+1} - \gamma B_{m_0+1}\right) p^2 + \left(\beta-\gamma\right)\left(a_{m_0}+1\right) p \\ & + \left(a_n A_{m_0+1} - a B_{m_0+1}\right) p \end{aligned}$$

Since p is a prime number and $0 < a_{m_0}+1 < p$, this results in $a - a_n \equiv 0 \pmod{p}$, what means $a \equiv a_n \equiv a_n^{[z+1]} \pmod{p}$.

Ad (ii): Here we distinguish the two sub-cases $a_n > 0$ and $a_n = 0$. First of all, we treat $a_n > 0$. By (3-33) and (3-34) we have the relation

(3-38) $$(\gamma p+a)(a_n+A_{n+1}p)\,p^n=(\beta p+a_n)\big((a_n+1)+A_{n+1}p\big)\,p^n$$

This can be transformed to

(3-39) $$a_n\big(a-(a_n+1)\big)=(\beta-\gamma)A_{n+1}p^2+(a_n-a)A_{n+1}p+\big(\beta(a_n+1)-\gamma a_n\big)p$$

Herein, the term a_n is relatively prime to p, since $0<a_n<p$ and p is prime. For that reason, we obtain $a-(a_n+1)\equiv 0\,(\mathrm{mod}\,p)$, consequently $a(n,z+1)=a\equiv(a_n+1)\equiv a_n^{[z+1]}\,(\mathrm{mod}\,p)$.

Now, we consider the case $m_0=n$ with $a_n=0$. By definition of m_n, then $m_n>m_0$ holds true. Further it follows by (3-27), (3-28) and (3-29)

(3-40) $$\begin{aligned} z+1&=1+\sum_{\mu=0}^{n-1}(p-1)p^{\mu}+\sum_{\mu=m_n}^{m}a_{\mu}p^{\mu}\\ &=p^n+A_{m_n}p^{m_n}\end{aligned}$$

Hence, $z+1$ suffices the preconditions of Lemma 3-2 (setting $m:=A_{m_n}p^{m_n-n-1}$ therein), i.e.,

(3-41) $$\binom{z+1}{p^n}=\binom{A_{m_n}p^{m_n}+p^n}{p^n}\equiv 1\,(\mathrm{mod}\,p)$$

Subsequently we obtain $a(n,z+1)\equiv 1\equiv a_n^{[z+1]}\,(\mathrm{mod}\,p)$.

Ad (iii): In this case (3-25) reads as follows

(3-42) $$(\gamma p+a)\Big(\big(p^{m_0-n}-1\big)+A_{m_0}p^{m_0-n}\Big)\,p^n=(\beta p+a_n)\big((a_{m_0}+1)+A_{m_0+1}p\big)\,p^{m_0}$$

This can be transformed to

(3-43) $$\begin{aligned} a\Big(\big(p^{m_0-n}-1\big)+A_{m_0}p^{m_0-n}\Big)&=(\beta p+a_n)\big((a_{m_0}+1)+A_{m_0+1}p\big)\,p^{m_0-n}\\ &\quad-\gamma\Big(\big(p^{m_0-n}-1\big)+A_{m_0}p^{m_0-n}\Big)p\end{aligned}$$

The term in parentheses on the left hand side evaluates to the remainder $-1\,(\mathrm{mod}\,p)$ evidently. The right hand side is a multiple of *p*. Thus we achieve $a(n,z+1)=a\equiv 0\equiv a_n^{[z+1]}(\mathrm{mod}\,p)$. □

The proposition formulated as Theorem 3-1 can be verified by an alternative approach too. In doing so we resort on the argumentation presented at the beginning of this section. There we discussed the products $(k)_l$. Then, if l is a power, say $l=p^n$, we obtain

$$(k)_{p^n} = \prod_{\nu=0}^{p^{n-1}-1} (k-\nu p)_p = \prod_{\nu=1}^{p^{n-1}} \left(k-p^n+\nu p\right)_p \tag{3-44}$$

This is a result of the following deduction

$$\begin{aligned}(k)_{p^n} &= k\left(k-1\right)\left(k-2\right)\cdot\ldots\cdot\left(k-p^n+1\right)\\ &= k\left(k-1\right)\left(k-2\right)\cdot\ldots\cdot\left(k-p+1\right)\cdot\\ &\cdot\left(k-p\right)\left(k-p-1\right)\left(k-p-2\right)\cdot\ldots\cdot\left(k-2p+1\right)\cdot\\ &\cdot\left(k-2p\right)\left(k-2p-1\right)\left(k-2p-2\right)\cdot\ldots\cdot\left(k-3p+1\right)\cdot\\ &\vdots\\ &\cdot\left(k-(p^{n-1}-1)p\right)\left(k-(p^{n-1}-1)p-1\right)\cdot\ldots\cdot\left(k-(p^{n-1}-1)p-p+1\right)\\ &= (k)_p\,(k-p)_p\,(k-2p)_p\cdot\ldots\cdot\left(k-(p^{n-1}-2)p\right)_p\left(k-(p^{n-1}-1)p\right)_p\end{aligned} \tag{3-45}$$

The binomial coefficient in discussion, $\binom{z}{p^n} = \frac{(z)_{p^n}}{p^n!}$, now can be rewritten as:

$$\binom{z}{p^n} = \frac{\prod_{\nu=1}^{p^{n-1}}\left(z-p^n+\nu p\right)_p}{\prod_{\nu=1}^{p^{n-1}}(\nu p)_p} \tag{3-46}$$

By the way: this representation leads to a nice identity for the product of the binomial coefficients involved. In fact we get $\binom{z}{p^n}\prod_{\nu=1}^{p^{n-1}}\binom{\nu p}{p} = \prod_{\nu=1}^{p^{n-1}}\binom{z-p^n+\nu p}{p}$.

For the denominator of (3-46) we can prove a proposition very analogous to that of Lemma 3-2.

Lemma 3-3

For prime numbers p and $m\in\mathbb{N}_0, n\in\mathbb{N}$, the following congruency holds true

$$p^{-\frac{p^n-1}{p-1}}\prod_{\nu=1}^{p^{n-1}}\left(z-p^n+\nu p\right)_p \equiv (-1)^{\frac{p^n-1}{p-1}}\left\lfloor\frac{z}{p^n}\right\rfloor \pmod p \tag{3-47}$$

Proof:

Let $F(n)$ denote the left hand side of (3-47). With respect to (3-2), we have

$$F(1) = p^{-\frac{p-1}{p-1}} \prod_{\nu=1}^{p^0} \left(z - p + \nu p\right)_p$$

$$= \frac{\left(z\right)_p}{p} \tag{3-48}$$

$$\equiv (-1)^{\frac{p-1}{p-1}\left\lfloor \frac{z}{p} \right\rfloor} \pmod p$$

for $n = 1$. For the induction step $n \mapsto n+1$, we conclude as follows:

$$F(n+1) = p^{-\frac{p^{n+1}-1}{p-1}} \prod_{\nu=1}^{p^n} \left(z - p^{n+1} + \nu p\right)_p$$

$$= p^{-\frac{p^{n+1}-1}{p-1}} p^{p^n} \prod_{\nu=1}^{p^n} \frac{\left(z - p^{n+1} + \nu p\right)_p}{p} \tag{3-49}$$

$$\equiv p^{-\frac{p^{n+1}-1}{p-1}} p^{p^n} \prod_{\nu=1}^{p^n} (-1)^{\left\lfloor \frac{z}{p} - p^n + \nu \right\rfloor}$$

$$\equiv p^{-\frac{p^{n+1}-1}{p-1}} p^{p^n} \prod_{\nu=1}^{p^n} (-1) \cdot \prod_{\nu=1}^{p^n} \left(\left\lfloor \frac{z}{p} \right\rfloor - p^n + \nu \right) \pmod p$$

Herein, the last step can be performed as a consequence of (3-2) again. It follows

$$F(n+1) \equiv (-1)^{p^n} \; p^{-\frac{p^n-1}{p-1}} \prod_{\nu=1}^{p^n} \left(\left\lfloor \frac{z}{p} \right\rfloor - p^n + \nu \right)$$

$$\equiv (-1)^{p^n} \; p^{-\frac{p^n-1}{p-1}} \prod_{\nu=1}^{p^{n-1}} \left(\left\lfloor \frac{z}{p} \right\rfloor - p^n + \nu p \right)_p \tag{3-50}$$

$$\equiv (-1)^{p^n} \; (-1)^{\frac{p^n-1}{p-1}\left\lfloor \frac{1}{p^n}\left\lfloor \frac{z}{p} \right\rfloor \right\rfloor} \pmod p$$

Due to $\left\lfloor \frac{1}{p^n}\left\lfloor \frac{z}{p} \right\rfloor \right\rfloor = \left\lfloor \frac{z}{p^{n+1}} \right\rfloor$ we come to the necessary conclusion in order to confirm the induction step.

$$F(n+1) \equiv (-1)^{\frac{p^{n+1}-1}{p-1}\left\lfloor \frac{z}{p^{n+1}} \right\rfloor} \pmod p \tag{3-51}$$

□

Thus, Theorem 3-1 is a consequence of (3-46), (3-47) and (3-17) (setting $m = 0$ there). In fact, we get

$$\binom{z}{p^n} = \frac{p^{-\frac{p^n-1}{p-1}} \cdot \prod_{\nu=1}^{p^{n-1}} \left(z - p^n + \nu p\right)_p}{p^{-\frac{p^n-1}{p-1}} \cdot \prod_{\nu=1}^{p^{n-1}} (\nu p)_p}$$

(3-52)

$$\equiv \frac{(-1)^{\frac{p^n-1}{p-1}\left\lfloor \frac{z}{p^n} \right\rfloor}}{(-1)^{\frac{p^n-1}{p-1}}}$$

$$\equiv \left\lfloor \frac{z}{p^n} \right\rfloor \pmod p$$

This is the desired result compliant with Theorem 3-1 because of $a_n \equiv \left\lfloor \frac{z}{p^n} \right\rfloor \pmod p$. □

Incidentally, the assertion made in Theorem 3-1 cannot be extended to general natural bases. This can be seen in the following way: Let $p > 1$ be a non-prime radix and suppose that q is the minimal prime factor of p. Based on the definition $z := p + q$, thereafter we have the canonical base-*p* representation $z = 1 \cdot p^1 + q \cdot p^0$, particularly $a_1 = 1$. Therewith we have

$$\binom{z}{p^1} = \binom{p+q}{p} = \binom{p+q}{q} = \frac{p+q}{q}\binom{p+q-1}{q-1}$$

For the binomial coefficient on the right it exists an integer number α such that

$$\binom{p+q-1}{q-1} = \frac{(p+q-1)\cdot\ldots\cdot(p+2)(p+1)}{(q-1)!}$$

$$= \frac{(\alpha p + (q-1)!)}{(q-1)!}$$

Plainly, if $q = 2$ then $\binom{p+q-1}{q-1} = p+1$. According to the precondition, $(q-1)!$ and p are relatively prime, provided $q > 2$. Since $\frac{(\alpha p + (q-1)!)}{(q-1)!}$ is an integer, it follows that $(q-1)!$ is a factor of α. Therefore $\alpha' := \frac{\alpha}{(p-1)!}$ is an integer too. So that, in both cases ($q = 2$ and $q > 2$) we find

$$\binom{z}{p^1} = \frac{p+q}{q} \cdot (\alpha' p + 1)$$

which implies $\binom{z}{p^1} \equiv \frac{p}{q} + 1 \neq 1 = a_1 \pmod{p}$. As a result, the proposition of Theorem 3-1 cannot be applied to non-prime radixes. □

Moreover, we can use the main result of this section in order to determine the integer residue modulo a prime p of special binomial coefficients. If we consider $z := m + (k + lp)p^n = m + kp^n + lp^{n+1}$ with $k < p$ and $m < p^n$, then we obtain $\binom{m + kp^n + lp^{n+1}}{p^n} \equiv k \pmod{p}$ by Theorem 3-1.

In general we have $\binom{z}{p^n} = \frac{z}{p^n}\binom{z-1}{p^n - 1}$. By substitution of $z = (k + lp)p^n = kp^n + lp^{n+1}$, again with $k < p$, this leads to $\binom{(k+lp)p^n}{p^n} = (k + lp)\binom{(k+lp)p^n - 1}{p^n - 1}$. On account of Theorem 3-1 the left hand side is congruent to the residue class $k \pmod{p}$. This implies $\binom{(k+lp)p^n - 1}{p^n - 1} \equiv 1 \pmod{p}$, only provided $k > 0$. □