BINOMIAL COEFFICIENTS INVOLVING INFINITE POWERS OF PRIMES

DONALD M. DAVIS

ABSTRACT. If p is a prime (implicit in notation) and n a positive integer, let $\nu(n)$ denote the exponent of p in n, and $\mathrm{U}(n) = n/p^{\nu(n)}$, the unit part of n. If α is a positive integer not divisible by p, we show that the p-adic limit of $(-1)^{p\alpha e}\,\mathrm{U}((\alpha p^e)!)$ as $e \to \infty$ is a well-defined p-adic integer, which we call z_α. Note that if $p = 2$ or α is even, this can be thought of as $\mathrm{U}((\alpha p^\infty)!)$. In terms of these, we then give a formula for the p-adic limit of $\binom{ap^e+c}{bp^e+d}$ as $e \to \infty$, which we call $\binom{ap^\infty+c}{bp^\infty+d}$. Here $a \ge b$ are positive integers, and c and d are integers.

1. Statement of results.

Let p be a prime number, fixed throughout. The set $\mathbb{Z}_p$ of p-adic integers consists of expressions of the form $x = \sum_{i=0}^{\infty} c_i p^i$ with $0 \le c_i \le p-1$. The nonnegative integers are those x for which the sum is finite. The metric on $\mathbb{Z}_p$ is defined by $d(x, y) = 1/p^{\nu(x-y)}$, where $\nu(x) = \min\{i : \ c_i \ne 0\}$. (See, e.g., [3].) The prime p will be implicit in most of our notation.

If n is a positive integer, let $\mathrm{U}(n) = n/p^{\nu(n)}$ denote the unit factor of n (with respect to p). Our first result is as follows.

Theorem 1.1. *Let α be a positive integer which is not divisible by p. If $p^e > 4$, then*

$$\mathrm{U}((\alpha p^{e-1})!) \equiv (-1)^{p\alpha}\,\mathrm{U}((\alpha p^e)!) \mod p^e.$$

This theorem implies that

$$d\big((-1)^{p\alpha(e-1)}\,\mathrm{U}((\alpha p^{e-1})!), (-1)^{p\alpha e}\,\mathrm{U}((\alpha p^e)!)\big) \le 1/p^e,$$

from which the following corollary is immediate.

Corollary 1.2. *If α is as in Theorem 1.1, then $\lim_{e\to\infty}(-1)^{p\alpha e}\,\mathrm{U}((\alpha p^e)!)$ exists in $\mathbb{Z}_p$. We denote this limiting p-adic integer by z_α.*

If $p=2$ or α is even, then z_α could be thought of as $\mathrm{U}((\alpha p^\infty)!)$. It is easy for `Maple` to compute z_α mod p^m for m fairly large. For example, if $p=2$, then $z_1\equiv 1+2+2^3+2^7+2^9+2^{10}+2^{12} \mod 2^{15}$. This is obtained by letting C_n denote the mod 2^{n+1} reduction of $U(2^n!)$ and computing $C_1=1$, $C_2=3$, $C_3=C_4=C_5=C_6=11$, $C_7=C_8=139$, $C_9=651$, $C_{10}=C_{11}=1675$, and $C_{12}=C_{13}=C_{14}=5771$. Similarly, if $p=3$, then $z_1\equiv 1+2\cdot 3+2\cdot 3^2+2\cdot 3^4+3^6+2\cdot 3^7+2\cdot 3^8 \mod 3^{11}$. It would be interesting to know, as a future investigation, if there are algebraic relationships among the various z_α for a fixed prime p.

There are two well-known formulas for the power of p dividing a binomial coefficient $\binom{a}{b}$. (See, e.g., [4].) One is that

$$\nu\tbinom{a}{b}=\tfrac{1}{p-1}(d_p(b)+d_p(a-b)-d_p(a)),$$

where $d_p(n)$ denotes sum of the coefficients when n is written in p-adic form as above. Another is that $\nu\binom{a}{b}$ equals the number of carries in the base-p addition of b and $a-b$. Clearly $\nu\binom{ap^e}{bp^e}=\nu\binom{a}{b}$.

Our next result involves the unit factor of $\binom{ap^e}{bp^e}$. Here one of a or b might be divisible by p. For a positive integer n, let $z_n=z_{\mathrm{U}(n)}$, where $z_{\mathrm{U}(n)}\in\mathbb{Z}_p$ is as defined in Corollary 1.2.

Theorem 1.3. *Suppose $1\le b\le a$ and $\{\nu(a),\nu(b),\nu(a-b)\}=\{0,k\}$ with $k\ge 0$. Then*

$$\mathrm{U}\left(\binom{ap^e}{bp^e}\right)\equiv(-1)^{pck}\frac{z_a}{z_bz_{a-b}}\mod p^e,$$

where $c=\begin{cases} a & \text{if } \nu(a)=k,\\ b & \text{if } \nu(b)=k,\\ a-b & \text{if } \nu(a-b)=k.\end{cases}$

Note that since one of $\nu(a)$, $\nu(b)$, and $\nu(a-b)$ equals 0, at most one of them can be positive.

Since $\nu\binom{ap^e}{bp^e}$ is independent of e, we obtain the following immediate corollary.

Corollary 1.4. *In the notation and hypotheses of Theorem 1.3, in $\mathbb{Z}_p$*

$$\binom{ap^\infty}{bp^\infty}:=\lim_{e\to\infty}\binom{ap^e}{bp^e}=p^{\nu\binom{a}{b}}(-1)^{pck}\frac{z_a}{z_bz_{a-b}}.$$

Our final result analyzes $\binom{ap^\infty+c}{bp^\infty+d}$, where c and d are integers, possibly negative.

Theorem 1.5. *If a and b are as in Theorem 1.3, and c and d are integers, then in $\mathbb{Z}_p$*

$$\binom{ap^\infty+c}{bp^\infty+d} := \lim_{e\to\infty}\binom{ap^e+c}{bp^e+d} = \begin{cases} \binom{ap^\infty}{bp^\infty}\binom{c}{d} & c,d\ge 0,\\ \binom{ap^\infty}{bp^\infty}\binom{c}{d}\frac{a-b}{a} & c<0\le d,\\ \binom{ap^\infty}{bp^\infty}\binom{c}{c-d}\frac{b}{a} & c<0\le c-d,\\ 0 & \text{otherwise.}\end{cases}$$

Here, of course, $\binom{ap^\infty}{bp^\infty}$ is as in Corollary 1.4, and we use the standard definition that if $c\in\mathbb{Z}$ and $d\ge 0$, then

$$\tbinom{c}{d} = c(c-1)\cdots(c-d+1)/d!.$$

These ideas arose in extensions of the work in [1] and [2].

2. Proofs

In this section, we prove the three theorems stated in Section 1. The main ingredient in the proof of Theorem 1.1 is the following lemma.

Lemma 2.1. *Let α be a positive integer which is not divisible by p, and let e be a positive integer. Let $I_{\alpha,e} = \{i : \alpha p^{e-1} < i \le \alpha p^e\}$, and let S denote the multiset consisting of the least nonnegative residues mod p^e of $\mathrm{U}(i)$ for all $i \in I_{\alpha,e}$. Then every positive p-adic unit less than p^e occurs exactly α times in S.*

Proof. Let $W_{\alpha,e}$ denote the set of positive integers prime to p which are less than αp^e. Then our unit function $\mathrm{U}: I_{\alpha,e}\to W_{\alpha,e}$ has an inverse function $\phi: W_{\alpha,e}\to I_{\alpha,e}$ defined by $\phi(u)=p^t u$, where

$$t=\max\{i : p^i u\le \alpha p^e\}.$$

Note that $p^t u\in I_{\alpha,e}$ since $p^{t+1}u>\alpha p^e$ which implies $p^t u>\alpha p^{e-1}$. One easily checks that U and ϕ are inverse and hence bijective. Since reduction mod p^e from $W_{\alpha,e}$ to $W_{1,e}$ is an α-to-1 function, preceding it by the bijection U implies the result. □

Proof of Theorem 1.1. If $p^e>4$, the product of all p-adic units less than p^e is congruent to $(-1)^p$ mod p^e. (See, e.g., [4, Lemma 1], where the argument is attributed to Gauss.) The theorem follows immediately from this and Lemma 2.1, since, mod

p^e, $\mathrm{U}((\alpha p^e)!)/\,\mathrm{U}((\alpha p^{e-1})!)$ is the product of the elements of the multiset S described in the lemma. □

Proof of Theorem 1.3. Suppose $\nu(b)=0$ and $a=\alpha p^k$ with $k\ge 0$ and $\alpha=\mathrm{U}(a)$. Then, mod p^e,

$$\begin{aligned}\mathrm{U}\left(\binom{\alpha p^{e+k}}{bp^e}\right) &= \frac{\mathrm{U}((\alpha p^{e+k})!)}{\mathrm{U}((bp^e)!)\cdot\mathrm{U}(((a-b)p^e)!)}\\ &\equiv \frac{(-1)^{p\alpha(e+k)}z_a}{(-1)^{pbe}z_b\cdot(-1)^{p(a-b)e}z_{a-b}}\\ &= (-1)^{pak}\frac{z_a}{z_bz_{a-b}},\end{aligned}$$

as claimed. Here we have used Theorem 1.1 and the notation introduced in Corollary 1.2. Also we have used that either $p=2$ or $a\equiv\alpha$ mod 2. A similar argument works if $\nu(b)=k>0$ (and $\nu(a)=0$), or if $\nu(a-b)=k>0$ (and $\nu(a)=\nu(b)=0$). □

Our proof of Theorem 1.5 uses the following lemma.

Lemma 2.2. *Suppose f is a function with domain $\mathbb{Z}\times\mathbb{Z}$ which satisfies Pascal's relation*

$$f(n,k)=f(n-1,k)+f(n-1,k-1) \tag{2.3}$$

for all n and k. If $f(0,d)=A\delta_{0,d}$ for all $d\in\mathbb{Z}$ and $f(c,0)=Ar$ for all $c<0$, then

$$f(c,d)=\begin{cases}A\binom{c}{d} & c,d\ge 0,\\ A\binom{c}{d}r & c<0\le d,\\ A\binom{c}{c-d}(1-r) & c<0\le c-d,\\ 0 & \textit{otherwise.}\end{cases}$$

The proof of this lemma is straightforward and omitted. It is closely related to work in [5] and [6], in which binomial coefficients are extended to negative arguments in a similar way. However, in that case (2.3) does not hold if $n=k=0$.

Proof of Theorem 1.5. Fix $a\ge b>0$. If $f_e(c,d):=\binom{ap^e+c}{bp^e+d}$, where e is large enough that $ap^e+c>0$ and $bp^e+d>0$, then (2.3) holds for f_e. If, as $e\to\infty$, the limit exists for two terms of this version of (2.3), then it also does for the third, and (2.3) holds for the limiting values, for all $c,d\in\mathbb{Z}$. The theorem then follows from Lemma 2.2 and (2.4) and (2.5) below, using also that if $d<0$, then $\binom{ap^e}{bp^e+d}=\binom{ap^e}{(a-b)p^e+|d|}$, to which (2.4) can be applied.

If $d > 0$, then

$$\binom{ap^e}{bp^e+d} = \binom{ap^e}{bp^e}\frac{((a-b)p^e)\cdots((a-b)p^e-d+1)}{(bp^e+1)\cdots(bp^e+d)} \to 0 \tag{2.4}$$

in $\mathbb{Z}_p$ as $e \to \infty$, since it is p^e times a factor whose p-exponent does not change as e increases through large values.

Let $c = -m$ with $m > 0$. Then

(2.5)

$$\binom{ap^e-m}{bp^e} = \binom{ap^e}{bp^e}\frac{((a-b)p^e)\cdots((a-b)p^e-m+1)}{ap^e\cdots(ap^e-m+1)} \to \binom{ap^\infty}{bp^\infty}\frac{a-b}{a},$$

in $\mathbb{Z}_p$ as $e \to \infty$, since

$$\frac{((a-b)p^e-1)\cdots((a-b)p^e-m+1)}{(ap^e-1)\cdots(ap^e-m+1)} \equiv 1 \mod p^{e-[\log_2(m)]}.$$

Here we have used that if $t < e$ and v is not divisible by p, then $\frac{(a-b)p^e-vp^t}{ap^e-vp^t} \equiv 1 \mod p^{e-t}$. □

References

[1] D. M. Davis, For which p-adic integers x can $\sum_k \binom{x}{k}^{-1}$ be defined?, *J. Comb. Number Theory* (forthcoming). Available at `http://arxiv.org/1208.0250`.

[2] —, Divisibility by 2 of partial Stirling numbers, *Funct. Approx. Comment. Math.* (forthcoming). Available at `http://arxiv.org/1109.4879`.

[3] F. Q. Gouvea, *p-adic Numbers: an Introduction*, Springer-Verlag, Berlin, Heidelberg, 1993.

[4] A. Granville, Binomial coefficients modulo prime powers, *CMS Conf. Proc* **20** (1997) 253–275.

[5] P. J. Hilton, J. Pederson, Extending the binomial coefficients to preserve symmetry and pattern, *Comput. Math. Appl.* **17** (1989) 89–102.

[6] R. Sprugnoli, Negation of binomial coefficients, *Discrete Math.* **308** (2008) 5070–5077.

Department of Mathematics, Lehigh University, Bethlehem, PA 18015

dmd1@lehigh.edu