SOME CONGRUENCES FOR BINOMIAL COEFFICIENTS

Carl S. Weisman

1. INTRODUCTION

Let p be a prime number. For integers m, and $n > 0$, and $s > 0$, denote by $M_s(m, n)$ the sum $\sum (-1)^{n-i}\binom{n}{i}$ of alternating binomial coefficients, restricted to those i which are congruent to m modulo p^s. Many results about continuous p-adic-valued functions on the p-adic integers come down to statements about the numbers $M_s(m, n)$. The author has shown that

$$(*) \qquad \operatorname{ord} M_s(m, n) \geq [n/p^{s-1}(p-1)] - 1$$

for all m. Here ord r denotes the exponent to which p divides r, and $[\cdot]$ is the integer-part function. The present note gives more precise information about the congruence properties of the $M_s(m, n)$ modulo powers of p. It is shown that, for fixed m and s, there is equality in (*) for infinitely many n; more specifically,

(i) *if* $k \geq 1$ *and* $n > kp^{s-1}(p-1) + p^{s-1} - 1$, *then* $\operatorname{ord} M_s(m, n) > k - 1$ *for all* m;

(ii) *if* $k \geq 1$, *then* $M_s(m, kp^{s-1}(p-1) + p^{s-1} - 1) \equiv (-p)^{k-1} \pmod{p^k}$ *for every* m.

These results are then applied to obtain a new characterization of uniformly Lipschitz p-adic-valued functions.

2. PRELIMINARY LEMMAS

In this section, p denotes a fixed prime.

LEMMA 1. *Let the integers* a_{in} *be defined by the identity*

$$\binom{py}{i} = \sum_n a_{in}\binom{y}{n}.$$

If $p \nmid a_{in}$, *then* $i = pn$.

Proof. One has $a_{in} = \sum_{j=0}^{n} (-1)^{n-j}\binom{n}{j}\binom{pj}{i}$. Fix n and let X be an indeterminate. Then $\sum_{i=0}^{n} a_{in}X^i = \sum_{j=0}^{n} (-1)^{n-j}\binom{n}{j}\sum_{i=0}^{pj}\binom{pj}{i}X^i = ((X+1)^p - 1)^n$. Comparing coefficients yields the lemma.

LEMMA 2. *If* $s \geq 2$ *and* $1 \leq i < p^{s-1}(p-1)$, *then* $\sum_{j=1}^{p-1}\binom{p^{s-1}j}{i}$ *is divisible by* p. *If, in addition,* $i < p^{s-2}(p-1)$, *then* $\sum_{j=1}^{p-1}\binom{p^{s-1}j}{i}$ *is divisible by* p^2.

Received November 24, 1976.

Michigan Math. J. 24 (1977).

Proof. Take $s = 2$. The first statement is automatic if $p \nmid i$. If $i = p\ell$ with $0 < \ell < p - 1$, then, modulo p, one has $\sum_{j=1}^{p-1} \binom{pj}{p\ell} \sum_{j=1}^{p-1} \binom{j}{\ell} = \binom{p}{\ell+1} \equiv 0$. If $0 < i < p - 1$, then $\sum_{j=1}^{p-1} \binom{pj}{i} = \sum_{j=1}^{p-1} \sum_{k=1}^{i} c_k p^k j^k$, where each c_k is p-integral. Now $\sum_{j=1}^{n} j^k = (n+1) Q_k(n)/(k+1)!$, where Q_k is a polynomial with integer coefficients. Therefore, $\sum_{j=1}^{p-1} \binom{pj}{i} = p^2 \sum_{k=1}^{i} c_k p^{k-1} Q_k(p-1)/(k+1)!$, and the last sum is p-integral; thus the second statement follows for $s = 2$.

Now assume $s > 2$. Again, the first statement is automatic if $p \nmid i$. If $i = p\ell$ with $0 < \ell < p^{s-2}(p-1)$, one has, modulo p, $\sum_{j=1}^{p-1} \binom{p^{s-1}j}{p\ell} \equiv \sum_{j=1}^{p-1} \binom{p^{s-2}j}{\ell}$, so that the first statement follows by induction on s.

Assume $i < p^{s-2}(p-1)$. In the notation of Lemma 1, we have

$$\sum_{j=1}^{p-1} \binom{p^{s-1}j}{i} = \sum_n a_{in} \sum_{j=1}^{p-1} \binom{p^{s-2}j}{n}.$$

Evidently, $a_{in} = 0$ if $n > i$. Thus, if $a_{in} \neq 0$, then $n < p^{s-2}(p-1)$, so that $\sum_{j=1}^{p-1} \binom{p^{s-2}j}{n}$. If a_{in} is not also divisible by p, then, according to Lemma 1, one has $n = i/p < p^{s-3}(p-1)$. Thus the final statement of the present lemma also follows by induction.

The familiar Vandermonde convolution formula, $\binom{n+n'}{i} = \sum_{j=0}^{i} \binom{n}{j}\binom{n'}{i-j}$, yields easily the similar identity $M_s(m, n+n') = \sum_{j=0}^{p^s-1} M_s(j, n) M_s(m-j, n')$.

LEMMA 3. *If* $p \neq 2$ *and* $k \geq 2$, *then* $\operatorname{ord} M_s(m, kp^s - 1) \geq k$ *for any* m.

Proof. Assume $0 \leq m < p^s$. Then since evidently $M_s(0, p^s) = 0$, one has

$$\begin{aligned} M_s(m, 2p^s - 1) &= \sum_{j=0}^{p^s-1} M_s(j, p^s - 1) M_s(m-j, p^s) \\ &= \sum_{j=0}^{m-1} (-1)^{p^s-1-j} \binom{p^s-1}{j} (-1)^{p^s-m-j} \binom{p^s}{m-j} \\ &\quad + \sum_{j=m+1}^{p^s-1} (-1)^{p^s-1-j} \binom{p^s-1}{j} (-1)^{p^s-p^s-m+j} \binom{p^s}{p^s+m-j} \\ &= p^s \sum_{j=0}^{m-1} (-1)^{m+1} \binom{p^s-1}{j} \binom{p^s-1}{m-j-1} (m-j)^{-1} \\ &\quad + p^s \sum_{j=m+1}^{p^s-1} (-1)^m \binom{p^s-1}{j} \binom{p^s-1}{j-m-1} (j-m)^{-1}. \end{aligned}$$

Now if $j < p^s$, then $\binom{p^s-1}{j} \equiv (-1)^j \pmod p$. Hence one has, modulo p^2,

$$M_s(m, 2p^s - 1) \equiv \sum_{j=0}^{m-1} p^s/(m-j) - \sum_{j=m+1}^{p^s-1} p^s/(j-m) \equiv \sum_{0<r<p^s} p^s/r \equiv 0 .$$

This begins an induction on k. To complete it, simply notice that

$$M_s(m, (k+1)p^s - 1) = \sum_{j=0}^{p^s-1} M_s(j, p^s) M_s(m-j, kp^s - 1)$$

$$= \sum_{j=1}^{p^s-1} (-1)^{j-1} \binom{p^s}{j} M_s(m-j, kp^s - 1) .$$

A polynomial $f(X) = \sum_{i=0}^{k-1} A_i X^i$ with p-integral rational coefficients will be said to be *overdetermined* if $A_0 \equiv 1 \pmod p$ and $A_i \equiv 0 \pmod{p^{i+1}}$ for $i > 0$. If f is overdetermined, then for any polynomial g with p-integral coefficients, and for each k, the coefficient of X^k in $f(X)g(pX)$ will be congruent modulo p^{k+1} to that in $g(pX)$. The set of overdetermined polynomials is carried into itself by any linear change of variables with p-integral coefficients. When regarded as elements of $(\mathbb{Z}/p^t\mathbb{Z})[X]$, the overdetermined polynomials form a group under multiplication.

If the degree of f is less than p, it is easy to see that f is overdetermined if and only if $f(0) \equiv 1 \pmod p$, and $\sum_{j=0}^{q} (-1)^{q-j} \binom{q}{j} f(j) \equiv 0 \pmod{p^{q+1}}$ for $1 \leq q \leq \deg f$. If r runs through a complete set of representatives for the units modulo p, then the polynomial $\prod_r (1 + pX/r)$, when truncated at degree $p - 2$, is overdetermined.

LEMMA 4. *Let* $s \geq 1$ *and* $2 < k < p$. *Then there is an overdetermined polynomial* $g_{sk}(X)$, *such that, for* $0 \leq j \leq k - 1$,

$$g_{sk}(j) \equiv \binom{kp^s - 1}{p^s - 1} \binom{(k-j)p^s - 1}{p^s - 1}^{-1} \pmod{p^k} .$$

Proof. It is sufficient to show that the polynomial $\binom{p^sX - 1}{p^s - 1}$ is congruent modulo p^k to an overdetermined polynomial. But

$$\binom{p^sX - 1}{p^s - 1} = \prod_{r=1}^{p^s-1} \frac{p^s(X-1) + r}{r} = \prod_{t=0}^{s-1} \prod_{\substack{1 \leq d < p^{s-t} \\ p \nmid d}} \left(1 + \frac{p^{s-t}}{d}(X-1)\right) .$$

The coefficient of each $(X-1)^i$ is evidently divisible by p^i; since $k < p$, therefore, the polynomial may be truncated at degree $p - 2$ without disturbing it modulo p^k. But, as remarked in the preceding paragraph, that yields an overdetermined polynomial.

PROPOSITION 5. *Let* $p \neq 2$, *and for* $2 \leq k \leq p - 1$, *let* $f_k(X)$ *be the unique* *polynomial of degree at most* $k - 1$, *such that* $f_k(j) = \binom{kp^s}{jp^s} / \binom{k}{j}$ *for* $0 \le j \le k - 1$. *Then* f_k *is overdetermined.*

Proof. For $k = 2$, since $f_2(0) = 1$, it is only necessary to show that $\binom{2p^s}{p^s} / \binom{2}{1} \equiv 1 \pmod{p^2}$. But $\binom{2p^s}{p^s} \binom{2}{1} = \binom{2p^s - 1}{p^s - 1} = \binom{2p^s - 1}{p^s}$, which, by Lemma 3, is congruent to $\binom{2p^s - 1}{0}$ modulo p^2.

For $k > 2$, notice first that

$$\sum_{j=0}^{k-1} (-1)^{k-1-j} \binom{k-1}{j} \binom{kp^s}{jp^s} / \binom{k}{j} = \sum_{j=0}^{k-1} (-1)^{k-1-j} \binom{kp^s - 1}{jp^s}$$

$$= M_s(0, kp^s - 1) \equiv 0 \pmod{p^k},$$

by Lemma 3.

On the other hand, if $0 \le j \le k - 2$, then one finds

$$\frac{\binom{kp^s}{jp^s}}{\binom{k}{j}} = \frac{\binom{(k-1)p^s}{jp^s}}{\binom{k-1}{j}} \binom{kp^s - 1}{p^s - 1} \binom{(k-j)p^s - 1}{p^s - 1}^{-1},$$

so that $f_k(j) \equiv f_{k-1}(j) g_{sk}(j) \pmod{p^k}$. Thus in calculating $\sum_{j=0}^{q} (-1)^{q-j} \binom{q}{j} f_k(j)$ modulo p^{q+1} for $q < k - 1$, we may replace f_k by $f_{k-1} g_{sk}$. But this latter, by induction and Lemma 4, is an overdetermined polynomial.

LEMMA 6. *Assume that for some* m_0, *there is a greatest integer* n^*, *such that* $kp^{s-1}(p - 1) \le n^* < (k + 1)p^{s-1}(p - 1)$, *and such that* $\operatorname{ord} M_s(m_0, n^*) = k - 1$. *Then* $\operatorname{ord} M_s(m, n^*) = k - 1$ *for all* m.

Proof. Applying the orthogonality relations

$$\sum_{j=0}^{m} (-1)^{j-m} \binom{m}{j} \binom{j}{i - \ell} = \delta_{m,i-\ell},$$

together with the Vandermonde convolution, yields the identity, for $m \ge 0$, $M_s(m_0 - m, n^*) = \sum_{j=0}^{m} \binom{m}{j} M_s(m_0, n^* + j)$. Now if $n^* + j \ge (k + 1)p^{s-1}(p - 1)$, it follows that $\operatorname{ord} M_s(m_0, n^* + j) \ge [(n^* + j)/p^{s-1}(p - 1)] - 1 \ge k$. If

$$n^* < n^* + j < (k + 1)p^{s-1}(p - 1),$$

then, by the maximality of n^*, it follows that $\operatorname{ord} M_s(m_0, n^* + j) > k - 1$. Therefore, $M_s(m_0 - m, n^*) \equiv M_s(m_0, n^*) \pmod{p^k}$.

3. THE CASE $p = 2$

PROPOSITION 7. *If* $k \geq 2$ *and* $s \geq 2$, *then*

$$M_s(m, 2^{s-1}(k+1) - 1) \equiv 2M_s(m - 2^{s-2}, 2^{s-1}k - 1) \pmod{2^k}, \quad \textit{for all } m.$$

Proof.
$$M_s(m, 2^{s-1}(k+1) - 1) = \sum_{j=0}^{2^s-1} M_s(j, 2^{s-1}) M_s(m - j, 2^{s-1}k - 1)$$
$$= \sum_{j=0}^{2^{s-1}} (-1)^j \binom{2^{s-1}}{j} M_s(m - j, 2^{s-1}k - 1).$$

Now each of the numbers $M_s(m - j, 2^{s-1}k - 1)$ is divisible by 2^{k-2}. Thus to calculate modulo 2^k, we may drop all j such that $2 \leq \operatorname{ord} \binom{2^{s-1}}{j} = s - 1 - \operatorname{ord} j$. Thus, modulo 2^k,

$$M_s(m, 2^{s-1}(k+1) - 1) \equiv M_s(m, 2^{s-1}k - 1)$$
$$+ \binom{2^{s-1}}{2^{s-2}} M_s(m - 2^{s-2}, 2^{s-1}k - 1) + M_s(m - 2^{s-1}, 2^{s-1}k - 1)$$
$$= M_{s-1}(m, 2^{s-1}k - 1) + \binom{2^{s-1}}{2^{s-2}} M_s(m - 2^{s-2}, 2^{s-1}k - 1).$$

But $\operatorname{ord} M_{s-1}(m, 2^{s-1}k - 1) \geq 2k - 2 \geq k$, and $\binom{2^{s-1}}{2^{s-2}} \equiv 2 \pmod 4$, whence the result.

COROLLARY 8. *If* $k \geq 2$ *and* $s \geq 2$, *then* $\operatorname{ord} M_s(m, 2^{s-1}k - 1) = k - 2$, *for all* m.

Proof. One has $M_s(0, 2^s - 1) = -1$. This, together with Lemma 6, begins the induction on k. Proposition 7, together with Lemma 6, completes it.

4. THE CASE $p \neq 2$

PROPOSITION 9. *Let* ω *be a primitive* p*-th root of unity. Then, in* $\mathbb{Z}_p[\omega]$, *one has* $(\omega - 1)^{p(p-1)} \equiv -p^p \pmod{p^{p+1}}$.

Proof. The element $\omega - 1$ satisfies the equation

$$0 = ((X+1)^p - 1)/X = \sum_{i=0}^{p-1} \binom{p}{i+1} X^i.$$

Thus $(\omega - 1)^{p-1} - \sum_{i=0}^{p-2} \binom{p}{i+1} (\omega - 1)^i = -p - p(\omega - 1)u$, where u is integral. Thus

$$(\omega - 1)^{p(p-1)} = -p^p - p^p \sum_{\ell=1}^{p} \binom{p}{\ell} (\omega - 1)^\ell u^\ell \equiv -p^p - p^p (\omega - 1)^p u^p \pmod{p^{p+1}},$$

since all other $\binom{p}{\ell}$ are divisible by p. But $(\omega - 1)^p$ is also divisible by p, so that $p^p(\omega - 1)^p u^p \equiv 0 \pmod{p^{p+1}}$, as required.

PROPOSITION 10. *Let* $s \geq 2$ *and let* ω *be a primitive* p^s*-th root of unity. Then, in* $\mathbb{Z}_p[\omega]$, *one has* $(\omega - 1)^{p^s(p-1)} \equiv -p^p \pmod{p^{p+1}}$.

Proof. The element $\omega - 1$ is a root of the polynomial

$$\sum_{j=0}^{p-1} (X+1)^{p^{s-1}j} = \sum_{i=0}^{p^{s-1}(p-1)} \sum_{j=0}^{p-1} \binom{p^{s-1}j}{i} X^i$$

so that $(\omega - 1)^{p^{s-1}(p-1)} = -p - u$, where $u = \sum_{i=1}^{p^{s-1}(p-1)-1} (\omega - 1)^i \sum_{j=1}^{p-1} \binom{p^{s-1}j}{i}$. One has $\operatorname{ord} u \geq \inf_{0<i<p^{s-1}(p-1)} \left\{\operatorname{ord} \sum_{j=1}^{p-1} \binom{p^{s-1}j}{i} + i/p^{s-1}(p-1)\right\}$.

Now by Lemma 2, it follows that, for $0 < i < p^{s-2}(p-1)$, one has

$$\operatorname{ord} \sum_{j=1}^{p-1} \binom{p^{s-1}j}{i} + i/p^{s-1}(p-1) > 2 > 1 + 1/p\,.$$

If $p^{s-2}(p-1) \leq i < p^{s-1}(p-1)$, one has $\operatorname{ord} \sum_{j=1}^{p-1}\binom{p^{s-1}j}{i} + i/p^{s-1}(p-1) \geq 1 + i/p$. Thus $\operatorname{ord} u \geq 1 + 1/p$.

Consequently,

$$\operatorname{ord}\left\{(\omega - 1)^{p^s(p-1)} - (-p)^p\right\} = \operatorname{ord} \sum_{\ell=1}^{p} \binom{p}{\ell} (-p)^{p-\ell}(-u)^{\ell}$$

$$\geq \inf_{1\leq \ell \leq p} \left\{\operatorname{ord}\binom{p}{\ell} + p - \ell + \ell + \ell/p\right\} = p+1\,,$$

as required.

In the propositions that follow, s will be fixed, and we shall abbreviate $N(m, k) = M_s(m, kp^{s-1}(p-1))$.

THEOREM 11. *Let* $s \geq 1$. *Then* $N(0, p) - N((p-1)p^{s-1}, p) \equiv -p^p \pmod{p^{p+1}}$. *If* $0 \leq r < p^{s-1}$ *and* $0 \leq j < p - 1$, *but* $r + j > 0$, *then*

$$N(r + jp^{s-1}, p) \equiv N(r + (p-1)p^{s-1}, p) \pmod{p^{p+1}}\,.$$

Proof. Let ω be a primitive p^s-th root of unity. Then a basis for $\mathbb{Z}_p[\omega]$ over $\mathbb{Z}_p$ is provided by $\{\omega^{r+jp^{s-1}}: 0 \leq r < p^{s-1},\ 0 \leq j < p-1\}$, and the coefficient of $\omega^{r+jp^{s-1}}$ in $(\omega - 1)^{p^s(p-1)}$ is $N(r + jp^{s-1}, p) - N(r + (p-1)p^{s-1}, p)$.

On the other hand, if we expand $(\omega - 1)^{p^s(p-1)} = \sum_{i=0}^{p^{s-1}(p-1)-1} C_i (\omega - 1)^i$, we have, by Propositions 9 and 10, that $C_0 \equiv -p^p \pmod{p^{p+1}}$, and $C_i \equiv 0 \pmod{p^{p+1}}$ for $i > 0$. But the coefficient of ω^n in $\sum_{i=0}^{p^{s-1}(p-1)-1} C_i (\omega - 1)^i$ is, *a priori*, equal to $\sum_{i=n}^{p^{s-1}(p-1)-1} (-1)^{i-n}\binom{i}{n} C_i$. This, together with the congruences for C_i, yields the theorem.

THEOREM 12. *Let* $k \geq 1$ *and* $n \geq kp^{s-1}(p-1)$. *Then for all* m, *one has* $M_s(m, np^s(p-1)) \equiv -p^p M_s(m, n) \pmod{p^{k+p}}$.

Proof. $M_s(m, np^s(p-1)) \sum_{\ell=0}^{p^s-1} N(\ell, p) M_s(m-\ell, n)$. Now for all ℓ, one has that $M_s(m-\ell, n)$ is divisible by p^{k-1}. This together with Theorem 11 yields, modulo p^{k+p},

$$M_s(m, np^s(p-1)) + p^p M_s(m, n)$$

$$\equiv \sum_{r=0}^{p^{s-1}-1} \sum_{j=0}^{p-1} N(r+(p-1)p^{s-1}, p) M_s(m-r-jp^{s-1}, n)$$

$$= \sum_{r=0}^{p^{s-1}-1} N(r+(p-1)p^{s-1}, p) \sum_{j=0}^{p-1} M_s(m-r-jp^{s-1}, n).$$

If $s = 1$, then $\sum_{j=0}^{p-1} M_s(m-r-jp^{s-1}, n) = \sum_{i=0}^{n} (-1)^{n-i}\binom{n}{i} = 0$. If $s > 1$, then $\sum_{j=0}^{p-1} M_s(m-r-jp^{s-1}, n) = M_{s-1}(m-r, n)$, which is divisible by p^{kp-1}. Since each $N(r+(p-1)p^{s-1}, p)$ is divisible by p^{p-1}, and since

$$kp - 1 + p - 1 \geq k + p,$$

the theorem follows.

THEOREM 13. *Let* $k \geq 1$. *Then* $M_s(0, kp^{s-1}(p-1) + p^{s-1} - 1) \equiv (-p)^{k-1} \pmod{p^k}$, *and* $M_s(0, n) \equiv 0 \pmod{p^k}$, *for all* $n > kp^{s-1}(p-1) + p^{s-1} - 1$.

Proof. Using an induction beginning with Lemma 3, one shows easily that if $n \geq kp^s - 1$, then $M_s(m, n) \equiv 0 \pmod{p^k}$ for all m. Thus for the present theorem, we may consider only those $n < kp^s - 1$. Moreover, it is sufficient to prove the theorem when $1 \leq k \leq p$; for Theorem 12 will provide an induction.

For $k = 1$, we have $M_s(0, p^s - 1) = 1$ and, if $p^s - 1 < n < 2p^s - 1$, then $M_s(0, n) = (-1)^n - (-1)^n\binom{n}{p^s} \equiv 0 \pmod{p}$.

Now let $k = p$ and let $s > 1$. Then by Theorem 11, if $0 \leq \ell < p - 1$, we have, modulo p^{p+1},

$$M_s(\ell p^{s-1}, n) \equiv -p^p M_s(\ell p^{s-1}, n - p^s(p-1))$$
$$+ \sum_{r=0}^{p^{s-1}-1} N(r+(p-1)p^{s-1}, p) \sum_{j=0}^{p-1} M_s(p^{s-1} - r - jp^{s-1}, n - p^s(p-1))$$

$$= -p^p M_s(\ell p^{s-1}, n - p^s(p-1))$$
$$+ \sum_{r=0}^{p^{s-1}-1} N(r+(p-1)p^{s-1}, p) M_{s-1}(-r, n - p^s(p-1)).$$

Summing these, we obtain, modulo p^{p+1},

$$-p^p M_{s-1}(0, n - p^s(p-1)) + p \sum_{r=0}^{p^{s-1}-1} N(r + (p-1)p^{s-1}, p) M_{s-1}(-r, n - p^s(p-1)) \equiv M_{s-1}(0, n) .$$

But if $n \geq p^s(p-1) + p^{s-1} - 1$, this last number is divisible by p^{p^2}. Also, by the case $k = 1$ for $s - 1$, we have $M_{s-1}(0, n - p^s(p-1)) \equiv 0 \pmod p$ for

$$n > p^s(p-1) + p^{s-1} - 1;$$

and $M_{s-1}(0, p^{s-1} - 1) = 1$.

Therefore, $\sum_{r=0}^{p^{s-1}-1} N(r + (p-1)p^{s-1}, p) M_{s-1}(-r, n - p^s(p-1))$ is congruent to $p^{p-1} \pmod{p^p}$ if $n = p^s(p-1) + p^{s-1} - 1$, and is congruent to 0 if n is greater. But this sum is congruent to $M_s(0, n)$ modulo p^p.

Now assume $s = 1$ and $k = p$. If $n > p(p-1)$, then, modulo p^{p+1},

$$M_1(0, n) \equiv -p^p M_1(0, n - p(p-1)) + \sum_{j=0}^{p-1} N(p-1, p) M_1(j, n - p(p-1))$$

$$= -p^p M_1(0, n - p(p-1)) .$$

If $n = p(p-1)$, we have, modulo p^{p+1}, $0 = \sum_{j=0}^{p-1} N(j, p) \equiv -p^p + pN(p-1, p)$, so that $N(p-1, p) \equiv p^{p-1} \pmod{p^p}$, so also $N(0, p) \equiv p^{p-1} \pmod{p^p}$.

If $2 < k < p$, and $0 \leq j < k$, notice that

$$\binom{n}{jp^s} = \frac{\binom{kp^s}{(k-j)p^s}\binom{(k-j)p^s}{kp^s - n}}{\binom{kp^s}{kp^s - n}} = \binom{k-1}{j} \frac{\binom{kp^s}{jp^s}}{\binom{k}{j}} \frac{\binom{(k-j)p^s - 1}{kp^s - n - 1}}{\binom{kp^s - 1}{kp^s - n - 1}}$$

$$= \binom{k-1}{j} \frac{\binom{kp^s}{jp^s}}{\binom{k}{j}} h_1(p^2 j) h_2(j),$$

where h_1 is a polynomial with p-integral coefficients and

$$h_2(X) = \prod_{\substack{1 \leq bp^{s-1} < kp^s - n \\ p \nmid b}} (1 - (p/kp - b)X) .$$

In the notation of Proposition 5, let $G(X)$ be a polynomial of degree at most $k - 1$ that is congruent modulo p^k to $f_k(X) h_1(p^2 X) h_2(X)$, and let A_{k-1} be its coefficient of X^{k-1}. Then, as is well known,

$$(k-1)!\,A_{k-1} = \sum_{j=0}^{k-1} (-1)^{k-1-j}\binom{k-1}{j} G(j) \equiv (-1)^{k-1-n} M_s(0, n) \pmod{p^k}.$$

But A_{k-1} is congruent modulo p^k to the coefficient of X^{k-1} in $h_2(X)$. That coefficient is 0 if $n > kp^{s-1}(p-1) + p^{s-1} - 1$; while if $n = kp^{s-1}(p-1) + p^{s-1} - 1$, it is $p^{k-1} \prod_{b=1}^{k-1} (b - kp)^{-1}$, which is $\equiv p^{k-1}/(k-1)! \pmod{p^k}$.

COROLLARY 14. *Let* $k \geq 1$. *Then for all* m,

$$M_s(m, kp^{s-1}(p-1) + p^{s-1} - 1) \equiv (-p)^{k-1} \pmod{p^k}.$$

If $n > kp^{s-1}(p-1) + p^{s-1} - 1$, *then* $M_s(m, n) \equiv 0 \pmod{p^k}$ *for all* m.

Proof. By the proof of Lemma 6 and by Theorem 13, one has, for

$$n^* = kp^{s-1}(p-1) + p^{s-1} - 1$$

and for any m, that $M_s(m, n^*) \equiv M_s(0, n^*) \pmod{p^k}$. Since

$$M_s(m, n+1) = M_s(m, n) - M_s(m-1, n),$$

the second assertion follows from the first.

COROLLARY 15. *Let* $k \geq 1$, *and abbreviate* $n_k = (k-1)p^{s-1}(p-1) + p^{s-1} - 1$. *Let* A *be the square matrix of size* $p^{s-1}(p-1)$ *whose* (i, j)*th entry is*

$$p^{-k+1} M_s(p^{s-1} - 1 + i, n_k + j).$$

Then the entries of A *and of its inverse are* p-*integral.*

Proof. The p-integrality of the entries of A is contained in Theorem 13. Let R_i be the i-th row of A, and perform the row operation replacing each R_i but the last by $\sum_{\ell=i}^{p^{s-1}(p-1)} M_s(-p^{s-1} - \ell, p^{s-1}(p-1) - i) R_\ell$. Then since the remaining $M_s(-p^{s-1} - \ell, p^{s-1}(p-1) - i)$ are zero, the new (i, j)th entry is

$$p^{-k+1} \sum_{\ell=0}^{p^s-1} M_s(-p^{s-1} - \ell, p^{s-1}(p-1) - i) M_s(p^{s-1} - 1 + \ell, n_k + j)$$

$$= p^{-k+1} M_s(-1, n_k + p^{s-1}(p-1) + j - i).$$

This p-integral number is $\equiv (-1)^{k-1} \pmod{p}$ when $i = j$, and $\equiv 0 \pmod{p}$ when $i < j$. Thus the determinant of A is $\equiv 1 \pmod{p}$.

Notice that the proofs of Corollaries 14 and 15 work as well when $p = 2$, by using Proposition 7 and Corollary 8.

5. AN APPLICATION

We shall consider here continuous functions from the p-adic integers to a complete valued extension field K of the p-adic numbers; the (exponential) valuation ord of K will be normalized by ord $p = 1$.

There are two popular ways of giving an "orthonormal expansion" of such a function f(y). One is Mahler's interpolation series $\sum a_n \binom{y}{n}$ [2, Chapter 6]. The other is van der Put's expansion $\sum b_m \chi_m(y)$ [3, Section 5]. Here, $\chi_0(y)$ is the characteristic function of the set of y with ord $y > 0$. If $m > 0$, $\chi_m(y)$ is the characteristic function of the set of y with ord $(y - m) > [\log_p m]$. The two expansions are related by $b_0 = a_0$, and, for $0 < n < p^s$,

$$a_n = M_1(0, n) b_0 + \sum_{t=1}^{s} \sum_{m=p^{t-1}}^{p^t -1} M_t(m, n) b_m .$$

It is not difficult [1] to show that the function f(y) is uniformly Lipschitz if and only if $\inf \{\text{ord } a_n - [\log_p n]\} > -\infty$.

THEOREM 16. f(y) *is uniformly Lipschitz if and only if*

$$\inf \{\text{ord } b_m - [\log_p m]\} > -\infty .$$

Proof. For $k \geq 1$ and $t \geq 1$, let $n_k(t) = (k - 1) p^{t-1}(p - 1) + p^{t-1} - 1$. Notice that for $s > t$, one has $n_k(s) = n_{k'}(t)$, with $k' = (k - 1) p^{s-t} + 1 + (p^{s-t} - 1)/(p - 1)$.

It follows from Corollary 15 that for any elements b_m of K, $p^{t-1} \leq m < p^t$, one has

$$\inf_{n_k(t) < n \leq n_{k+1}(t)} \text{ord} \sum_{m=p^{t-1}}^{p^t-1} M_t(m, n) b_m = k - 1 + \inf_{p^{t-1} \leq m < p^t} \text{ord } b_m .$$

Assume that $\sum a_n \binom{y}{n} = \sum b_m \chi_m(y)$ and that there is a constant B such that ord $a_n \geq B + [\log_p n]$ for all $n \geq 1$. We may assume, by subtracting a constant, that $a_0 = b_0 = 0$. But then $B \leq \inf_{n_1(1) < n \leq n_2(1)} \text{ord } a_n = \inf_{1 \leq m < p} \text{ord } b_m$.

Assume for induction that for all $1 \leq m < p^{s-1}$ one has ord $b_m \geq B + [\log_p m]$. Then for $p^{t-1} \leq m < p^t < p^s$ and $n_1(s) < n \leq n_2(s)$, one has

$$\text{ord } M_t(m, n) \geq B + t - 1 + (p^{s-t} - 1)(p - 1) > B + s - 1 .$$

Since ord $\sum_{t=1}^{s} \sum_{m=p^{t-1}}^{p^t -1} M_t(m, n) b_m \geq B + s - 1$ whenever $n_1(s) < n \leq n_2(s)$, it follows for each such n that ord $\sum_{m=p^{s-1}}^{p^s -1} M_s(m, n) b_m \geq B + s - 1$. Thus ord $b_m \geq B + s - 1$ whenever $[\log_p m] = s - 1$.

Now assume ord $b_m \geq B + [\log_p m]$. Again we may assume $a_0 = b_0 = 0$, and then, for $n_1(s) < n \leq n_2(s)$, we have

$$\begin{aligned} \text{ord } a_n &\geq \inf_{\substack{1 \leq t < s \\ p^{t-1} \leq m < p^t}} \{\text{ord } M_t(m, n) + \text{ord } b_m\} \\ &\geq \inf \{(p^{s-t} - 1)(p - 1) + B + t - 1\} = B + s - 1 . \end{aligned}$$

REFERENCES

1. E. Helsmoortel, *Comportement local des fonctions continues sur un compact régulier d'un corps local.* C.R. Acad. Sci. Paris Sér. A 271 (1970), 546-548.

2. K. Mahler, *Introduction to* p-*adic numbers and their functions.* Cambridge Tracts in Mathematics, No. 64, Cambridge University Press, London-New York, 1973.

3. A. C. M. van Rooij and W. H. Schikhof, *Non-archimedean analysis.* Nieuw Arch. Wisk. (3) 19 (1971), 120-160.

4. C. Weisman, *On* p-*adic differentiability.* J. Number Theory 9 (1977), 79-86.

Department of Mathematics
University of Rochester
Rochester, New York 14627