A NEW APPLICATION OF THE SCHUR DERIVATE

GORDON OVERHOLTZER

Fermat's theorem in elementary number theory states that if p is a rational prime, a an integer,

$$a^p \equiv a \pmod{p}.$$

Hence

$$a^{p^{n+1}} \equiv a^{p^n} \pmod{p^{n+1}}$$

or

$$(0,\ 1) \qquad (a^{p^{n+1}} - a^{p^n})/p^{n+1}$$

is a rational, hence a p-adic, integer.

By introducing as the derivate, Δa_n, of a sequence $\{a_n\}$ with respect to the number p the expression

$$(0,\ 2) \qquad \Delta a_n = (a_{n+1} - a_n)/p^{n+1},$$

I. Schur[1] in 1933 generalized Fermat's theorem. The Fermat theorem states that the first Schur derivate of the sequence $\{a^q\}$ with $q=p^n$, (0, 1), is integral. Schur proved the generalization that, if a is prime to p, not only the first derivate, but the higher Schur derivates up to the $(p-1)$st are integral (in the p-adic or rational sense). Zorn[2] in 1936 extended this result by proving that all Schur derivates of $\{a^q\}$ with $q=p^n$ are p-adically bounded, hence convergent, and discussing the p-adic function, $\lim_{n\to\infty} \Delta^m a^q$, where $q=p^n$.

It is a fact[3] of elementary number theory that the sum of the kth (k a positive or negative integer or zero) powers of the rational integers less than and prime to p^n (p a rational prime, n a positive integer) is divisible by p^n if $p-1$ does not divide k or by p^{n-1} if $p-1$ divides k. The quotient of the division of such a sum by p^n,

$$(0,\ 3) \qquad S[n,\ x^k] = \sum_{i=1}^{q}{}' i^k/p^n,$$

Presented to the Society, November 25, 1944; received by the editors July 6, 1944.

[1] Preuss. Akad. Wiss. Sitzungsber. (1933) p. 145.

[2] Ann. of Math. vol. 38 (1937) pp. 451–464.

[3] For a recent proof see H. Gupta, Proceedings of the Indian Academy of Sciences, Section A, vol. 13 (1944) pp. 85–86. His theorem is stated for even k, but the evenness of k is not used. Note that all concepts used are defined for negative k and the same proof holds. Classic results in number theory are Wolstenholme's theorem and Leudesdorf's generalization which yield divisibility by p^{2n} for $k=-1$, $p>3$.

(where $q=p^n$ and the prime on the summation sign indicates summation over i, $(i, p)=1$) is then a p-adic integer or has at most a denominator of p.

The present paper studies the p-adic properties of the sequence $\{S[n, x^k]\}$. It is proved that the sequence is p-adically convergent. A p-adic function, $\lim_{n\to\infty} S[n, x^k]$, may be defined for rational integers, and an elementary expression for this function for positive k given in terms of Bernoullian numbers. All the Schur derivates of this sequence, $\Delta^m S[n, x^k]$, are p-adically bounded, hence p-adically convergent. The limit of $\Delta^m S[n, x^k]$ is given in terms of the p-adic function, $\lim_{n\to\infty} S[n, x^{k-m}]$.

The quotients

$$Q[n, x^k] = \sum_{i=1}^{q}{}' i^k/p^{2n}, \tag{0, 4}$$

where $q=p^n$, are p-adically bounded for k odd. Moreover $\{Q[n, x^k]\}$ is p-adically convergent for k odd. The function $\lim_{n\to\infty} Q[n, x^k]$ (k odd) is given in terms of $\lim_{n\to\infty} S[n, x^{k-1}]$.

If we write

$$T[n, g(x)] = \sum_{i=1}^{q}{}' g(i), \qquad S[n, g(x)] = T[n, g(x)]/p^n, \tag{0, 5}$$

where $q=p^n$, it is evident that the results concerning $\{S[n, x^k]\}$ extend to $\{S[n, g(x)]\}$ if $g(x)$ is a polynomial. It is proved also that these results extend to $S[n, f(x)]$ where $f(x)$ is the power series

$$f(x) = \sum_{j=e}^{\infty} a_j x^j$$

and the valuation of a_j approaches zero as j approaches ∞. Moreover

$$\lim_{n\to\infty} S[n, f(x)] = \sum_{j=e}^{\infty} a_j \lim_{n\to\infty} S[n, x^j].$$

The results for $\{S[n, x^k]\}$ are deduced as consequences of general formulas for $\Delta^m S[n, g(x)]$, Schur derivates of the sequence of sums of the values of $g(x)$ for x less than and prime to p^n divided by p^n. The sums are over a special set of values, a reduced residue set modulo p^n; sums over other sets of values of x might be studied. For example, the function might be summed over integers congruent to c modulo p and less than p^n. The formulas of this paper could be used in this special case by setting $g(x)=0$ in the other residue classes. In fact, the methods of this paper treat the values belonging to a particular residue class modulo p together as a part of the whole sum.

1. Power series representations of the Schur derivates. It will be convenient first to consider the sum of the values of a function, $g(x)$, for the integers less than and prime to p^n, p a rational prime. The results of this section will be applied to the special case $g(x)=x^k$ and theorems concerning the p-adic convergence of $\{S[n, x^k]\}$ and the Schur derivates of this sequence will be proved.

Assume that $g(x)$ is a function defined for p-adic integers and $g(x)$ can be represented by power series[4]

$$g(x) = \sum_{j=0}^{\infty} g^{(j)}(a)(x-a)^j/j!, \qquad a = 1, 2, \cdots, p-1,$$

p-adically convergent if $\phi(x-a)<1$, ϕ the valuation function. Note that the power series about different a are independent. A consequence of this analyticity condition is that $g(x)$ can be developed about any point in the circle of convergence, and the series will converge for any point in the original circle to the same limit. Since each of the power series can be differentiated term by term, $g^{(k)}(x)$ is a function satisfying the analyticity conditions imposed on $g(x)$ in this paragraph.

Assume also that $S[n, g^{(k)}(x)]$ is p-adically bounded uniformly, that is, if $\phi(p)=\delta$,

$$\phi\{S[n, g^{(k)}(x)]\} \leqq \delta^N, \qquad n = 1, 2, 3, \cdots, \tag{1, 1}$$

where N is independent of k.

The power series of $g(x)$ will be used to express $S[n+1, g(x)]$ and consequently $\Delta S[n, g(x)]$ as an infinite series in $S[n, g^{(\alpha)}(x)]$. Now

$$T[n+1, g(x)] = \sum_{i=1}^{r}{}' g(i) = \sum_{j=1}^{q}{}' \sum_{\nu=0}^{p-1} g(j+\nu p^n),$$

where $r=p^{n+1}$ and $q=p^n$,

$$T[n+1, g(x)] = \sum_{j=1}^{q}{}'\sum_{\nu=0}^{p-1} \{g(j) + (\nu p^n)g'(j) + (\nu p^n)^2 g''(j)/2! + \cdots\}.$$

Summing out on ν and writing $b(k)=\sum_{\nu=0}^{p-1}\nu^k=T[1, x^k]$, we obtain

[4] For a discussion of the power series of $g(x)$ and proof of the properties cited, see Schöbe, *Beiträge zur Funktionentheorie in nichtarchimedisch bewerteten Körpern*, Inaugural Dissertation, Halle, 1930, pp. 17–19. However, we use only such of his theorems as are capable of an easy proof.

$$\begin{aligned} T[n+1, g(x)] &= \sum_{j=1}^{q}{}' [pg(j) + b(1)p^n g'(j) + b(2)p^{2n}g''(j)/2! + \cdots] \\ &= p \sum_{j=1}^{q}{}' g(j) + b(1)p^n \sum_{j=1}^{q}{}' g'(j) \\ &\quad + b(2)p^{2n} \sum_{j=1}^{q}{}' g''(j)/2! + \cdots \\ &= pT[n, g(x)] + b(1)p^n T[n, g'(x)] \\ &\quad + b(2)p^{2n}T[n, g''(j)]/2! + \cdots , \end{aligned}$$

$$(1,\ 2) \qquad T[n+1, g(x)] - pT[n, g(x)] = \sum_{\rho=1}^{\infty} \frac{b(\rho)p^{\rho n}}{\rho!} T[n, g^{(\rho)}(x)].$$

Divide (1, 2) by p^{n+1} and obtain

$$(1,\ 3) \quad S[n+1, g(x)] - S[n, g(x)] = \frac{1}{p} \sum_{\rho=1}^{\infty} \frac{b(\rho)p^{\rho n}}{\rho!} S[n, g^{(\rho)}(x)].$$

Substitution of (1, 3) into the definition of $\Delta S[n, g(x)]$ gives

$$\Delta S[n, g(x)] = \frac{1}{p} \sum_{\rho=1}^{\infty} \frac{b(\rho)p^{\rho n}}{\rho!} S[n, g^{(\rho)}(x)]/p^{n+1},$$

$$(1,\ 4) \qquad \Delta S[n, g(x)] = \frac{1}{p^2} \sum_{\rho=1}^{\infty} \frac{b(\rho)p^{n(\rho-1)}}{\rho!} S[n, g^{(\rho)}(x)].$$

Write

$$(1,\ 5) \qquad L'(\rho) = p^{-2}b(\rho)/\rho!.$$

Since $g^{(k)}(x)$ is a function satisfying all the conditions imposed on $g(x)$, (1, 4) becomes

$$(1,\ 6) \qquad S[n, g^{(k)}(x)] = \sum_{\rho=1}^{\infty} L'(\rho)p^{n(\rho-1)}S[n, g^{(k+\rho)}(x)].$$

Note that the coefficients $L'(\rho)$ depend only on the summation index.

An estimate of the valuation of $L'(\rho)$ will be required for the investigation of the higher derivates. From (1, 5)

$$\phi[L'(\rho)] = \phi[p^{-2}b(\rho)/\rho!] = \phi(p^{-2})\phi[b(\rho)]\phi[1/\rho!].$$

If $\rho = \sum_{i=0}^{e} u_i p^i$, $0 \leq u_i < p$, the power of p in $\rho!$ is $(\rho - \sum_{i=0}^{e} u_i)/(p-1)$ and is, therefore, at most $\rho/(p-1)$. Hence

$$(1,\ 7) \qquad \phi[L'(\rho)] < \delta^{-2}\delta^{-\rho/(p-1)} = \delta^{-2-\rho/(p-1)}.$$

In general, an expression for $\Delta^{r+1}S[n, g(x)]$ as an infinite series in $S[n, g^{(\alpha)}(x)]$ may be obtained from a series for $\Delta^r S[n, g(x)]$ by substitution into the definition of $\Delta^{r+1}S[n, g(x)]$, algebraic manipulation, and rearrangement of a double series. A recursion formula for the coefficients of the series for $\Delta^{r+1}S[n, g(x)]$ in terms of the coefficients of $\Delta^r S[n, g(x)]$, $\Delta S[n, g(x)]$ results. Justification of the rearrangement of the double series requires an estimate of the valuation of the coefficients of $\Delta^r S[n, g(x)]$ and $\Delta S[n, g(x)]$. This estimate of the valuation of the coefficients is established by induction, using the recursion formula for the coefficients. To prove the possibility of representation of $\Delta^r S[n, g(x)]$ as an infinite series in $S[n, g^{(\alpha)}(x)]$ in the manner described, the results concerning the recursion formula and the valuation of the coefficients will be stated before it is evident how they are obtained.

(1, 8) THEOREM. *If $g(x)$ is a function defined for p-adic integers, and $g(x)$ may be expanded into power series about $a=1, 2, \cdots, p-1$, p-adically convergent if $\phi(x-a)<1$, and $S[n, g^{(k)}(x)]$ is uniformly p-adically bounded, then there exist coefficients $L^{(m)}(\alpha)$ independent of n and $g(x)$ such that*

$$\Delta^m S[n, g(x)] = \sum_{\alpha=m}^{\infty} L^{(m)}(\alpha) p^{n(\alpha-m)} S[n, g^{(\alpha)}(x)], \tag{1, 9}$$

$$L'(\gamma) = \frac{p^{-2}b(\gamma)}{\gamma!},$$

$$L^{(m+1)}(\gamma) = \sum\nolimits^{*m} p^{\alpha-m} L^{(m)}(\alpha) L'(\beta) + (p^{\gamma-m-1} - p^{-1}) L^{(m)}(\gamma),[5] \tag{1, 10}$$

$$\phi[L^{(m)}(\alpha)] < \delta^{-2m-\alpha/(p-1)}. \tag{1, 11}$$

The proof is by induction on m. For $m=1$, (1, 9) and (1, 11) become (1, 4) and (1, 7). The first formula of (1, 10) is (1, 5).

Assume (1, 9) and (1, 11) hold for $m \leqq r$. The truth of (1, 9) and (1, 11) for $m=1, r$ implies (1, 9) for $m=r+1$ and the recursion formula of (1, 10) for $m=r$. The recursion formula of (1, 10) for $m=r$ implies (1, 11) for $m=r+1$. Substitution of (1, 9) for $m=r$ into the definition of $\Delta^{r+1}S[n, g(x)]$ gives

[5] The composite superscript "$*m$" after a "$\sum$" shall indicate the summation condition $\alpha+\beta=\gamma$, $\beta \geqq 1$, $\alpha \geqq m$. The notations "$\sum^{*r}$" and "$\max^{*r}$" are to be interpreted correspondingly.

$$
\begin{aligned}
\Delta^{r+1}S[n, g(x)] &= \{\Delta^r S[n+1, g(x)] - \Delta^r S[n, g(x)]\}/p^{n+1} \\
&= \left\{ \sum_{\alpha=r}^{\infty} L^{(r)}(\alpha) p^{(n+1)(\alpha-r)} S[n+1, g^{(\alpha)}(x)] \right. \\
&\quad \left. - \sum_{\alpha=r}^{\infty} L^{(r)}(\alpha) p^{n(\alpha-r)} S[n, g^{(\alpha)}(x)] \right\} / p^{n+1} \\
&= \sum_{\alpha=r}^{\infty} L^{(r)}(\alpha) \{ p^{(n+1)(\alpha-r)} S[n+1, g^{(\alpha)}(x)] \\
&\quad - p^{(n+1)(\alpha-r)} S[n, g^{(\alpha)}(x)] + p^{(n+1)(\alpha-r)} S[n, g^{(\alpha)}(x)] \\
&\quad - p^{n(\alpha-r)} S[n, g^{(\alpha)}(x)] \} / p^{n+1} \\
&= \sum_{\alpha=r}^{\infty} L^{(r)}(\alpha) \{ p^{(n+1)(\alpha-r)} \Delta S[n, g^{(\alpha)}(x)] \\
&\quad + (p^{(n+1)(\alpha-r)} - p^{n(\alpha-r)}) S[n, g^{(\alpha)}(x)]/p^{n+1} \} \\
&= \sum_{\alpha=r}^{\infty} L^{(r)}(\alpha) \left\{ p^{(n+1)(\alpha-r)} \sum_{\beta=1}^{\infty} L'(\beta) p^{n(\beta-1)} S[n, g^{(\alpha+\beta)}(x)] \right. \\
&\quad \left. + (p^{(n+1)(\alpha-r)} - p^{n(\alpha-r)}) S[n, g^{(\alpha)}(x)]/p^{n+1} \right\}.
\end{aligned}
$$

The coefficient of $S[n, g^{(\gamma)}(x)]$ in $\Delta^{r+1}S[n, g(x)]$, after a formal rearrangement of terms, which will be justified later, is

$$
\begin{aligned}
&\textstyle\sum^{*r} L^{(r)}(\alpha) p^{(n+1)(\alpha-r)} L'(\beta) p^{n(\beta-1)} + (p^{(n+1)(\gamma-r)} - p^{n(\gamma-r)}) L^{(r)}(\gamma)/p^{n+1} \\
&= \textstyle\sum^{*r} p^{n(\alpha+\beta-r-1)+\alpha-r} L^{(r)}(\alpha) L'(\beta) + (p^{(n+1)(\gamma-r-1)} - p^{n(\gamma-r-1)-1}) L^{(r)}(\gamma) \\
&= p^{n[\gamma-(r+1)]} [\textstyle\sum^{*r} p^{\alpha-r} L^{(r)}(\alpha) L'(\beta) + (p^{\gamma-r-1} - p^{-1}) L^{(r)}(\gamma)].
\end{aligned}
$$

Writing

$$
(1, 12) \quad L^{(r+1)}(\gamma) = \textstyle\sum^{*r} p^{\alpha-r} L^{(r)}(\alpha) L'(\beta) + (p^{\gamma-r-1} - p^{-1}) L^{(r)}(\gamma),
$$

which is (1, 10) for $m=r$, we obtain

$$
(1, 13) \qquad \Delta^{r+1}S[n, g(x)] = \sum_{\gamma=r+1}^{\infty} L^{(r+1)}(\gamma) p^{n[\gamma-(r+1)]} S[n, g^{(\gamma)}(x)],
$$

since from (1, 10) for $m=r$, $L^{(r+1)}(i)=0$, $i=1, 2, \cdots, r$.

The validity of the rearrangement remains to be established. It suffices to show that the iterated series

$$
\sum_{\alpha=r}^{\infty} L^{(r)}(\alpha) p^{(n+1)(\alpha-r)} \sum_{\beta=1}^{\infty} L'(\beta) p^{n(\beta-1)} S[n, g^{(\alpha+\beta)}(x)]
$$

may be summed as

$$\sum_{\gamma=r+1}^{\infty} \left\{ \sum{}^{*r} L^{(r)}(\alpha) p^{(n+1)(\alpha-r)} L'(\beta) p^{n(\beta-1)} S[n, g^{(\alpha+\beta)}(x)] \right\}.$$

It is sufficient[6] to show that the valuation of the general term $p^{n(\alpha+\beta-r-1)+\alpha-r} L^{(r)}(\alpha) L'(\beta) S[n, g^{(\alpha+\beta)}(x)]$ becomes arbitrarily small for $\alpha+\beta$ sufficiently large. Using (1, 1) and our induction assumption (1, 11) for $m=1, r$,

$$\begin{aligned} \phi\{p^{n(\alpha+\beta-r-1)+\alpha-r} L^{(r)}(\alpha) L'(\beta) S[n, g^{(\alpha+\beta)}(x)]\} & \\ &\leqq \delta^{n(\alpha+\beta-r-1)+\alpha-r} \delta^{-2r-\alpha/(p-1)} \delta^{-2-\beta/(p-1)} \delta^{N} \\ &< \delta^{(\alpha+\beta)[n-1/(p-1)]-n(r+1)-r-2r-2+N} \\ &< \delta^{\epsilon} \end{aligned}$$

if $\alpha+\beta > (\epsilon+nr+n+3r+2-N)/[n-1/(p-1)]$. Hence the rearrangement is valid and (1, 10) for $m=r$, (1, 12), and (1, 9) for $m=r+1$, (1, 13) have been established.

Finally it must be established that (1, 11) is hereditary. By (1, 10) for $m=r$,

$$\begin{aligned} &\phi[L^{(r+1)}(\gamma)] \\ &\leqq \max\left\{\phi\left[\sum{}^{*r} p^{(\alpha-r)} L^{(r)}(\alpha) L'(\beta)\right], \phi\left[(p^{\gamma-r-1} - p^{-1}) L^{(r)}(\gamma)\right]\right\} \\ &\leqq \max\left\{\max{}^{*r} \left(\delta^{\alpha-r}\delta^{-2r-\alpha/(p-1)}\delta^{-2-\beta/(p-1)}, \delta^{-1}\delta^{-2r-\gamma/(p-1)}\right)\right\} \\ &= \max\left\{\max_{\alpha\geqq r} \left(\delta^{\alpha-r-2(r+1)-\gamma/(p-1)}\right), \delta^{-2r-1-\gamma/(p-1)}\right\} \\ &= \delta^{-2(r+1)-\gamma/(p-1)} \end{aligned}$$

which is (1, 11) for $m=r+1$. The induction is complete.

2. **The Schur derivates of x^k.** In this section the results of the previous section are applied to the special case of $g(x)=x^k$ (k a rational integer; positive, negative, or zero). Note that $g(x)=x^k$ is a function satisfying the conditions imposed on $g(x)$ in the preceding section. The function is defined for p-adic integers. The function x^k may be developed in power series by the binomial theorem. Finally

$$\phi\{S[n, x^k]\} \leqq \delta^{-1}, \tag{2, 1}$$

since $\sum_{i=1}^{\prime q} i^k$, where $q=p^n$, is divisible by p^n if $p-1$ does not divide k or by p^{n-1} if $p-1$ divides k.

The formula (1, 9) and the estimate of the valuation (1, 11) make it

[6] This rearrangement is an application of a more general theorem of Schöbe, loc. cit. p. 16.

possible to establish bounds for each Schur derivate $\Delta^m S[n, x^k]$.

$$\begin{aligned}\phi(\Delta^m S[n, x^k]) &= \phi\left\{\sum_{\alpha=m}^{\infty} L^{(m)}(\alpha) p^{n(\alpha-m)} S[n, (x^k)^{(\alpha)}]\right\} \\ &\leqq \max_{\alpha \geqq m} \phi\{L^{(m)}(\alpha) p^{n(\alpha-m)} S[n, (x^k)^{(\alpha)}]\} \\ &\leqq \max_{\alpha \geqq m} \delta^{-2m-\alpha/(p-1)+n(\alpha-m)-1} \\ &= \max_{\alpha \geqq m} \delta^{\alpha[n-1/(p-1)]-m(n+2)-1}.\end{aligned}$$

Since the exponent of δ in the valuation of the terms of $\Delta^m S[n, x^k]$ is a nondecreasing function of α, the first term ($\alpha = m$) has the maximum valuation. Hence

$$\phi(\Delta^m S[n, x^k]) \leqq \delta^{-2m-m/(p-1)-1}. \tag{2, 2}$$

Since the exponent of δ in (2, 2) is independent of n, it follows that

(2, 3) THEOREM. *All the Schur derivates $\Delta^m S[n, x^k]$ are p-adically bounded.*

If the mth derivate is bounded, the $(m-1)$st derivate is p-adically convergent. An immediate consequence of (2, 3) is

(2, 4) THEOREM. *All the Schur derivates $\Delta^m S[n, x^k]$ are p-adically convergent.*

In particular, since the first derivate $\Delta S[n, x^k]$ is bounded,

(2, 5) THEOREM. *$S[n, x^k]$ is p-adically convergent.*

The formula (1, 9) may also be used to obtain expressions for the p-adic limits of the Schur derivates. From the argument used in establishing (2, 3), it may be observed that all terms of $\Delta^m S[n, x^k] = \sum_{\alpha=m}^{\infty} L^{(m)}(\alpha) p^{n(\alpha-m)} S[n, (x^k)^{(\alpha)}]$ after the first have power of p at least

$$\begin{aligned}(m+1)[n - 1/(p-1)] - m(n+2) - 1 \\ = n - 2m - (m+1)/(p-1) - 1.\end{aligned}$$

Hence

$$\Delta^m S[n, x^k] = L^{(m)}(m) S[n, (x^k)^{(m)}] + p^{n-2m-(m+1)/(p-1)-1} R_n, \tag{2, 6}$$

where R_n is a p-adic integer. As n approaches ∞, the second term of the right member of (2, 6) approaches zero. Hence

$$(2, 7)\qquad \begin{aligned}\lim_{n\to\infty} \Delta^m S[n, x^k] &= \lim_{n\to\infty} L^{(m)}(m) S[n, (x^k)^{(m)}] \\ &= k(k-1)\cdots(k-m+1)L^{(m)}(m)\lim_{n\to\infty} S[n, x^{k-m}].\end{aligned}$$

From the Bernoulli numbers, an elementary expression for $\lim_{n\to\infty} S[n, x^k]$ for positive k may be derived. Summation over numbers relatively prime to p may be accomplished by summing over all integers and subtracting the sum over multiples of p. Then, setting $q = p^n$ and $s = p^{n-1}$,

$$T[n, x^k] = \sum_{i=1}^{q}{}' i^k = \sum_{i=1}^{q} i^k - \sum_{i=1}^{s} (pi)^k = \sum_{i=1}^{q-1} i^k - p^k \sum_{i=1}^{s-1} i^k.$$

For positive even k, introducing the Bernoulli numbers, B_i,

$$\begin{aligned}T[n, x^k] &= (p^n)^{k+1}/(k+1) - (p^n)^k/2 + \cdots + (-1)^{k/2-1}B_{k/2}p^n \\ &\quad - p^k[(p^{n-1})^{k+1}/(k+1) - (p^{n-1})^k/2 + \cdots \\ &\qquad\qquad + (-1)^{k/2-1}B_{k/2}p^{n-1}] \\ &= (-1)^{k/2-1}B_{k/2}p^n - p^k(-1)^{k/2-1}B_{k/2}p^{n-1} + S_n,\end{aligned}$$

where S_n has power of p at least $2(n-1)$ minus the maximum exponent of p in the denominators of the coefficients of $(p^n)^2, \cdots, (p^n)^{k+1}$, say $2n - c_k$, where c_k is independent of n. Then

$$S[n, x^k] \equiv (-1)^{k/2-1}B_{k/2}(1 - p^{k-1}) (\text{mod } p^{n-c_k}).$$

Hence, for k even,

$$(2, 8)\qquad \lim_{n\to\infty} S[n, x^k] = (-1)^{k/2-1}B_{k/2}(1 - p^{k-1}).$$

For positive odd k,

$$\begin{aligned}T[n, x^k] &= (p^n)^{k+1}/(k+1) - (p^n)^k/2 + \cdots \\ &\quad + (-1)^{(k-3)/2}kB_{(k-1)/2}(p^n)^2/2 \\ &\quad - p^k[(p^{n-1})^{k+1}/(k+1) - (p^{n-1})^k/2 + \cdots \\ &\qquad\qquad + (-1)^{(k-3)/2}kB_{(k-1)/2}(p^{n-1})^2/2].\end{aligned}$$

$T[n, x^k]$ has power of p at least $2(n-1)$ minus the maximum exponent of p in the denominators of the coefficients of $(p^n)^{k+1}, \cdots, (p^n)^2$, say $2n - c_k$, c_k independent of n. Hence

$$(2, 9)\qquad T[n, x^k] \equiv 0 \ (\text{mod } p^{2n-c_k}).$$

Then

$$S[n, x^k] \equiv 0 \pmod{p^{n-ck}}$$

and, for k odd,

$$\lim_{n\to\infty} S[n, x^k] = 0. \tag{2, 10}$$

3. **The quotients** Q. The congruence (2, 9) shows that, for positive odd k,

$$Q[n, x^k] = T[n, x^k]/p^{2n} \tag{3, 1}$$

is p-adically bounded, with

$$\phi(Q[n, x^k]) \leqq \delta^{-ck}.$$

The possibility of a theory concerning the p-adic properties of $\{Q[n, x^k]\}$ for odd k is suggested. We mention the following result.

(3, 2) THEOREM. *$Q[n, x^k] \equiv kS[n, x^{k-1}]/2 \pmod{p^n}$, k odd and p an odd prime.*

We prove this for positive k as follows: Since k is odd,

$$\begin{aligned}
\sum_{i=1}^{q}{}' i^k &= \sum_{i=1}^{q}{}'(p^n - i)^k \\
&= \sum_{i=1}^{q}{}' \sum_{\nu=0}^{k} \binom{k}{\nu} (p^n)^\nu(-i)^{k-\nu} \\
&= \sum_{i=1}^{q}{}' \{(-i)^k + p^n k(-i)^{k-1} \\
&\qquad\qquad + p^{2n}k(k-1)(-i)^{k-2}/2 + \cdots + (p^n)^k\} \\
&\equiv -\sum_{i=1}^{q}{}' i^k + p^n k \sum_{i=1}^{q}{}'(-i)^{k-1} \pmod{p^{3n}},
\end{aligned}$$

where $q = p^n$, since if k is odd, $k-2$ is not divisible by $p-1$, p an odd prime, and $\sum_{i=1}^{\prime q}(-i)^{k-2}$ is divisible by p^n. Hence

$$2T[n, x^k] \equiv p^n kT[n, x^{k-1}] \pmod{p^{3n}}.$$

Division by $2p^{2n}$ yields (3, 2).

Theorem (3, 2) yields immediately that, k odd,

$$Q[n, x^k] = kS[n, x^{k-1}]/2 + p^n I, \tag{3, 3}$$

I a p-adic integer. Hence $\{Q[n, x^k]\}$ is p-adically convergent, since each term of the right member of (3, 3) is convergent.

(3, 4) THEOREM. *For k odd, p an odd prime, $Q[n, x^k]$ is p-adically convergent, and*

$$\lim_{n\to\infty} Q[n, x^k] = k \lim_{n\to\infty} S[n, x^{k-1}]/2.$$

By (2, 8), for positive odd k,

$$\lim_{n\to\infty} Q[n, x^k] = k(-1)^{(k-1)/2-1}B_{(k-1)/2}(1 - p^{k-2})/2. \tag{3, 5}$$

4. Extension to functions defined by power series. The results of Theorems (2, 3), (2, 4), and (2, 5) extend immediately to $\Delta^m S[n, g(x)]$, if $g(x)$ is a polynomial. The object of this section is to extend these results to the case where $g(x)$ is a power series

$$f(x) = \sum_{i=e}^{\infty} a_i x_i, \tag{4, 1}$$

where e is any integer. A necessary and sufficient condition that $f(x)$ be defined for p-adic integers is that $\phi(a_i)\to 0$ as $i\to\infty$. If the coefficients a_i satisfy this condition, $f(x)$ is a function satisfying all the conditions imposed on $g(x)$ in §1. Now

$$\begin{aligned} S[n, f(x)] &= \sum_{i=1}^{q}{}' f(i)/p^n = \sum_{i=1}^{q}{}' \sum_{j=e}^{\infty} a_j i^j/p^n \\ &= \sum_{j=e}^{\infty} a_j \sum_{i=1}^{q}{}' i^j/p^n = \sum_{j=e}^{\infty} a_j S[n, x^j], \end{aligned}$$

where $q = p^n$. We wish to show that the limit can be taken term by term, that is,

$$\lim_{n\to\infty} S[n, f(x)] = \lim_{n\to\infty} \sum_{j=e}^{\infty} a_j S[n, x^j] = \sum_{j=e}^{\infty} a_j \lim_{n\to\infty} S[n, x^j]. \tag{4, 2}$$

To establish (4, 2), it is sufficient to show that

(4, 3) $\lim_{n\to\infty} a_j S[n, x^j]$ exists,

(4, 4) $\sum_{j=e}^{\infty} a_j S[n, x^j]$ converges uniformly in n, that is, for each $\epsilon > 0$, there exists an N such that $\phi(a_j S[n, x^j]) < \epsilon$ for $j \geqq N$, N independent of n.

The condition (4, 3) is satisfied by virtue of Theorem (2, 5) and the condition (4, 4) is satisfied from the condition on the coefficients a_j and the fact that $\phi(S[n, x^j]) \leqq \delta^{-1}$. Hence we have

(4, 5) THEOREM. *$\{S[n, f(x)]\}$ is p-adically convergent and*

$$(4, 6)\qquad \lim_{n\to\infty} S[n, f(x)] = \sum_{j=e}^{\infty} a_j \lim_{n\to\infty} S[n, x^j].$$

5. Sums of kth powers. This section will consider the sum of the kth powers of the positive rational integers congruent to one modulo p and less than p^n. Write

$$(5, 1)\qquad T_1[n, x^k] = \sum_{i=1, i\equiv p \pmod p}^{q} i^k,$$

where $q = p^n$. In this case k may be chosen a p-adic integer.

Since the residue class one is a subgroup of the cyclic group of a reduced residue set modulo p^n, it is cyclic and there exists a primitive root, r, generating the residue class modulo p^n. Then

$$T_1[n, x^k] \equiv r^k + r^{2k} + \cdots + r^{p^{n-1}k} \pmod{p^n}$$
$$\equiv r^k(1 - r^{kp^{n-1}})/(1 - r^k) \pmod{p^n}.$$

If $k = p^\mu \lambda$, $(\lambda, p) = 1$, then the power of p in $1 - r^{kp^{n-1}}$ is $\mu + n$ and the power of p in $1 - r^k$ is $\mu + 1$. Hence

$$(5, 2)\qquad T_1[n, x^k] \equiv 0 \pmod{p^{n-1}}.$$

If we write

$$(5, 3)\qquad S_1[n, x^k] = T_1[n, x^k]/p^{n-1},$$

$S_1[n, x^k]$ is a p-adic integer.

For other residue classes define, $(i_0, p) = 1$,

$$(5, 4)\qquad T_{i_0}[n, x^k] = \sum_{i=1, i\equiv i_0 \pmod p}^{q} i^k,$$

where $q = p^n$. Then

$$T_{i_0}[n, x^k] = \sum_{\nu=0}^{p^{n-1}-1} (i_0 + \nu p)^k = i_0^k \sum_{\nu=0}^{p^{n-1}-1} \left(1 + \frac{\nu}{i_0} p\right)^k$$
$$\equiv i_0^k \sum_{\nu=0}^{p^{n-1}-1} (1 + \nu p)^k \pmod{p^n} \equiv i_0^k T_1[n, x^k],$$

$$(5, 5)\qquad T_{i_0}[n, x^k] \equiv 0 \pmod{p^{n-1}},$$

since ν and ν/i_0 run through the same residue classes modulo p^n. Note that $T_{i_0}[n, x^k]$ is exactly divisible by p^{n-1}, that is, not divisible by p^n.

UNIVERSITY OF CALIFORNIA AT LOS ANGELES