[8] — *Einige neuere Bedingungen für die Existenz ungerader vollkommener Zahlen*, Journ. Reine Angew. Math. 192 (1953), pp. 24-34.

[9] Barkley Rosser, *Explicit bounds for some functions of prime numbers*, Amer. Journ. Math. 63 (1941), pp. 211-232.

[10] Karl Prachar, *Primzahlverteilung*, Berlin 1957.

Reçu par la Rédaction le 20. 3. 1960

ACTA ARITHMETICA
VI (1961)

Criteria for Kummer's congruences

by

L. Carlitz (Durham, N. C.)

1. Kummer ([2]) obtained the well-known congruence for the Euler numbers

$$\sum_{s=0}^{r}(-1)^s\binom{r}{s}E_{n+s(p-1)}\equiv 0\,(\mathrm{mod}\,p^r)\qquad (n\geqslant r,\ p>2)$$

by means of the following general result. Let p be a fixed prime $\geqslant 2$. Then if

$$\sum_{n=0}^{\infty}a_n\frac{x^n}{n!}=\sum_{k=0}^{\infty}A_k(e^x-1)^k, \tag{1.1}$$

where the a_n, A_k are integral $(\mathrm{mod}\,p)$, it follows that

$$\sum_{s=0}^{r}(-1)^s\binom{r}{s}a_{n+s(p-1)}\equiv 0\,(\mathrm{mod}\,p^r)\qquad (n\geqslant r). \tag{1.2}$$

Indeed since (1.1) is equivalent to

$$a_n=\sum_{k=0}^{n}A_kC_n^{(k)},\qquad \text{where}\qquad C_n^{(k)}=\sum_{j=0}^{k}(-1)^{k-j}\binom{k}{j}j^n,$$

we have

$$\sum_{s=0}^{r}(-1)^s\binom{r}{s}a_{n+s(p-1)}=\sum_{k=0}^{n+r(p-1)}A_k\sum_{s=0}^{r}(-1)^s\binom{r}{s}C_{n+s(p-1)}^{(k)}$$
$$=\sum_{k=0}^{n+r(p-1)}A_k\sum_{j=0}^{k}(-1)^{k-j}\binom{k}{j}j^n(1-j^{p-1})^r$$

and (1.2) follows by Fermat's theorem.

It is natural to ask whether the hypothesis in (1.1) that the A_k are integral $(\bmod p)$ can be weakened. We shall show that this is indeed the case. We prove below that (1.2) holds if and only if

$$\sum_{n=0}^{\infty} a_n \frac{x^n}{n!} = \sum_{k=0}^{\infty} A_k \frac{(e^x-1)^k}{k!},$$

where

$$(1.3) \qquad A_k \equiv 0 \ (\bmod p^{[k/p]});$$

it is assumed that the a_n are integral $(\bmod p)$.

The series e^x-1 seems to play a peculiar role in this result. However we show that if

$$g(x) = \sum_{n=1}^{\infty} c_n \frac{x^n}{n!},$$

where the c_n are integral $(\bmod p)$, $c_1 \not\equiv 0 \ (\bmod p)$ and

$$g(x) = \sum_{k=1}^{\infty} C_k \frac{f^k(x)}{k!},$$

where $f(x)$ is a fixed series whose coefficients satisfy (1.2), then the c_n satisfy the congruence

$$\sum_{s=0}^{r} (-1)^s \binom{r}{s} c_{n+s(p-1)} \equiv 0 \ (\bmod p^r) \qquad (n \geqslant r)$$

if and only if

$$C_k \equiv 0 \ (\bmod p^{[k/p]}).$$

Finally, we show that if we put

$$a_n = \sum_{j=0}^{N} j^n U_j^{(N)} \qquad (\text{all } N \geqslant n)$$

then the coefficients $U_j^{(N)}$ are uniquely determined and that (1.2) holds if and only if

$$k!\, U_k^{(k)} \equiv 0 \ (\bmod p^{[k/p]}).$$

2. We recall that a Hurwitz series ([1]) is one of the form

$$(2.1) \qquad f(x) = \sum_{0}^{\infty} a_n \frac{x^n}{n!},$$

where the a_n are integers. For brevity we denote by $\mathfrak{H}$ the set of all series (2.1) and by $\mathfrak{H}_p$ the set of series (2.1) in which the a_n are integral $(\bmod p)$, or, if we prefer, are p-adic integers. Then both $\mathfrak{H}$ and $\mathfrak{H}_p$ are closed with respect to addition and multiplication. Also if in (2.1) the leading coefficient $a_0 = 0$, Hurwitz showed that

$$(2.2) \qquad f^k(x) \equiv 0 \ (\bmod k!).$$

The statement

$$\sum_{0}^{\infty} a_n \frac{x^n}{n!} \equiv \sum_{0}^{\infty} b_n \frac{x^n}{n!} \ (\bmod m)$$

is equivalent to

$$a_n \equiv b_n \ (\bmod m) \qquad (n = 0, 1, 2, \ldots).$$

As a consequence of (2.2) it follows that if $f, g \in \mathfrak{H}$ (or $\mathfrak{H}_p$) then $f(g) \in \mathfrak{H}$ (or $\mathfrak{H}_p$). Morevoer if

$$(2.3) \qquad y = \sum_{n=1}^{\infty} a_n \frac{x^n}{n!} \qquad (a_1 = 1),$$

where the a_n are integral, then

$$x = \sum_{n=1}^{\infty} b_n \frac{y^n}{n!} \qquad (b_1 = 1),$$

where the b_n are integral. Thus for the special series (2.3) the inverse is also in $\mathfrak{H}$; a similar result holds for $\mathfrak{H}_p$.

Now put

$$(2.4) \qquad \mu(k) = \left[\frac{k}{p}\right] + \left[\frac{k}{p^2}\right] + \ldots, \qquad \nu(k) = \left[\frac{k}{p^2}\right] + \left[\frac{k}{p^3}\right] + \ldots,$$

where $[x]$ is the greatest integer function. Thus $p^{\mu(k)}$ is the highest power of p that divides $k!$

We shall require the following result.

THEOREM 1. *Put*

$$(e^x-1)^k = \sum_{n=k}^{\infty} C_n^{(k)} \frac{x^k}{n!}.$$

Then

$$(2.5) \qquad \sum_{s=0}^{r} (-1)^s \binom{r}{s} C_{n+s(p-1)}^{(k)} \equiv 0 \ (\bmod p^{r+\nu(k)}) \qquad (n \geqslant r).$$

Proof. By (2.2) and (2.4)

$$C_n^{(k)} \equiv 0 \pmod{p^{\mu(k)}}.$$

Hence if $r \leqslant k/p$, (2.5) is obviously true. We may accordingly assume that $r > k/p$.

Let $D = d/dx$. Then (2.5) is equivalent to

$$(D^p - D)^r (e^x - 1)^k \equiv 0 \pmod{p^{r+\nu(k)}}. \tag{2.6}$$

Now since

$$D(e^x-1)^k = k(e^x-1)^{k-1}e^x = k(e^x-1)^{k-1} + k(e^x-1)^k,$$

it follows at once that

$$D^n(e^x-1)^k = \sum_{j=0}^{n} a_j (e^x-1)^{k-j},$$

where the a_j are rational integers that depend on n and k. In particular, for $n = p$, we have

$$\begin{aligned} D^p(e^x-1)^k &= \sum_{s=0}^{k} (-1)^{k-s}\binom{k}{s} D^p e^{sx} = \sum_{s=0}^{k} (-1)^{k-s}\binom{k}{s} s^p e^{sx} \\ &= \sum_{s=0}^{k} (-1)^{k-s}\binom{k}{s} s^p \sum_{j=0}^{s}\binom{s}{j}(e^x-1)^j \\ &= \sum_{j=0}^{k}\binom{k}{j}(e^x-1)^j \sum_{s=j}^{k}(-1)^{k-s}\binom{k-j}{s-j} s^p \\ &= \sum_{j=0}^{p}\binom{k}{j}(e^x-1)^{k-j}\sum_{s=0}^{j}(-1)^s (k-s)^p. \end{aligned}$$

If we put

$$u_k = \frac{(e^x-1)^k}{k!}, \tag{2.7}$$

this becomes

$$D^p u_k = \sum_{j=0}^{p} \frac{u_{k-j}}{j!}\sum_{s=0}^{j}(-1)^s\binom{j}{s}(k-s)^p. \tag{2.8}$$

Since

$$\sum_{s=0}^{j}(-1)^s\binom{j}{s}s = j\sum_{s=1}^{j}(-1)^s\binom{j-1}{s-1} = 0 \qquad (j>1),$$

is follows that

$$\frac{1}{j!}\sum_{s=0}^{j}(-1)^s\binom{j}{s}(k-s)^p \equiv 0 \pmod{p} \qquad (1<j<p).$$

For $j = 1$ we have

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

while for $j = p$

$$\frac{1}{p!}\sum_{s=0}^{p}(-1)^s\binom{p}{s}(k-s)^p = 1.$$

Thus (2.8) becomes

$$D^p u_k = k^p u_k + u_{k-p} + \sum_{j=1}^{p-1} c_j u_{k-j},$$

where

$$c_1 \equiv 1, \quad c_j \equiv 0 \pmod{p} \quad (1<j<p).$$

Since

$$Du_k = ku_k + u_{k-1},$$

it follows that

$$(D^p - D)u_k = u_{k-p} + p\sum_{j=0}^{p-1} d_j u_{k-j}, \tag{2.9}$$

where the d_j are rational integers.

A second application of (2.9) yields

$$(D^p-D)^2 u_k = u_{k-2p} + p\sum_{j=0}^{p-1} d'_j u_{k-p-j} + p^2\sum_{j=0}^{p-1} d''_j u_{k-j},$$

where d'_j, d''_j are integral. Continuing in this way we get

$$(D^p-D)^r u_k = u_{k-rp} + \sum_{s=1}^{r} p^s \sum_{j=0}^{p-1} d_j^{(s)} u_{k-(r-s)p-j}, \tag{2.10}$$

where the $d_j^{(s)}$ are integral.

As noted above we may assume $pr > k$. Choose t so that

$$(r-t)p \leqslant k, \quad (r-t+1)p > k,$$

that is

$$t = r - \left[\frac{k}{p}\right]. \tag{2.11}$$

Then (2.10) reduces to

$$(D^p - D)^r u_k = \sum_{s=t}^{r} p^s \sum_{j=0}^{p-1} d_j^{(s)} u_{k-(r-s)p-j}.$$

Since $u_k \in \mathfrak{H}$ it follows that

$$(D^p - D)^r u_k \equiv 0 \pmod{p^t}.$$

Hence by (2.5) and (2.11)

$$(D^p - D)^r (e^x - 1)^k \equiv 0 \pmod{p^{r-[k/p]+\mu(k)}},$$

which is the same as (2.6).

This completes the proof of Theorem 1.

3. Let

$$f(x) = \sum_{n=0}^{\infty} a_n \frac{x^n}{n!} \tag{3.1}$$

be an arbitrary series in $\mathfrak{H}$ (or $\mathfrak{H}_p$). Since

$$x = \log\left((e^x - 1) + 1\right) = \sum_{k=1}^{\infty} \frac{(-1)^{k-1}}{k} (e^x - 1)^k,$$

it follows that

$$f(x) = \sum_{k=0}^{\infty} A_k \frac{(e^x - 1)^k}{k!} \qquad (A_0 = a_0), \tag{3.2}$$

where the A_k are integral. Thus an arbitrary $f(x)$ in $\mathfrak{H}$ (or $\mathfrak{H}_p$) will always be representable in the form (3.2).

Now assume that the A_k satisfy

$$A_k \equiv 0 \pmod{p^{[k/p]}} \qquad (k = 0, 1, 2, \ldots). \tag{3.3}$$

Applying the operator $(D^p - D)^r$ to both sides of (3.2) we get

$$(D^p - D)^r f(x) = \sum_{k=0}^{\infty} A_k (D^p - D)^r \frac{(e^x - 1)^k}{k!}. \tag{3.4}$$

By (2.6) we have

$$(D^p - D)^r (e^x - 1)^k \equiv 0 \pmod{p^{r-\nu(k)}}.$$

Hence for $r \geqslant k/p$

$$(D^p - D)^r \frac{(e^x - 1)^k}{k!} \equiv 0 \pmod{p^{r-[k/p]}};$$

using (3.3) this becomes

$$A_k (D^p - D)^r \frac{(e^x - 1)^k}{k!} \equiv 0 \pmod{p^r} \qquad (r \geqslant k/p). \tag{3.5}$$

On the other hand for all r

$$\frac{1}{k!} (e^x - 1)^k \in \mathfrak{H} \quad (\text{or } \mathfrak{H}_p)$$

and consequently

$$(D^p - D)^r \frac{(e^x - 1)^k}{k!} \in \mathfrak{H} \quad (\text{or } \mathfrak{H}_p).$$

Thus by (3.3) we get

$$A_k (D^p - D)^r \frac{(e^x - 1)^k}{k!} \equiv 0 \pmod{p^{[k/p]}} \tag{3.6}$$

for all k. Combining (3.5) with (3.6) it is clear that

$$\sum_{k=0}^{\infty} A_k (D^p - D)^r \frac{(e^x - 1)^k}{k!} \equiv 0 \pmod{p^r}. \tag{3.7}$$

Since

$$(D^p - D)^r f(x) = \sum_{s=0}^{r} (-1)^{r-s} \binom{r}{s} D^{r+s(p-1)} f(x)$$

$$= \sum_{n=0}^{\infty} \frac{x^n}{n!} \sum_{s=0}^{r} (-1)^{r-s} \binom{r}{s} a_{n+r+s(p-1)},$$

it follows from (3.4) and (3.7) that

$$\sum_{s=0}^{r} (-1)^s \binom{r}{s} a_{n+s(p-1)} \equiv 0 \pmod{p^r} \qquad (n \geqslant r). \tag{3.8}$$

We have therefore proved that (3.3) implies (3.8).

We assume now that (3.8) holds for all $n \geqslant r \geqslant 0$. Then (3.4) becomes

$$\sum_{k=0}^{\infty} A_k (D^p - D)^r \frac{(e^x-1)^k}{k!} \equiv 0 \pmod{p^r}. \tag{3.9}$$

Put

$$(e^x-1)^k = \sum_{n=k}^{\infty} C_n^{(k)} \frac{x^n}{n!}, \tag{3.10}$$

so that

$$C_n^{(k)} = \sum_{j=0}^{k} (-1)^{k-j} \binom{k}{j} j^n. \tag{3.11}$$

Since

$$C_n^{(k)} = 0 \qquad (k > n), \tag{3.12}$$

(3.9) implies

$$\sum_{k=0}^{N} \frac{1}{k!} A_k \sum_{s=0}^{r} (-1)^s \binom{r}{s} C_{n+s(p-1)}^{(k)} \equiv 0 \pmod{p^r} \qquad (n \geqslant r) \tag{3.13}$$

for all $N \geqslant n + r(p-1)$.

We now assume that (3.3) holds for $k < h$ and put

$$h = rp + r_0 \qquad (0 \leqslant r_0 < p).$$

In (3.13) take $n = r + r_0$, $N = h$. Since by (2.5)

$$\sum_{s=0}^{r} (-1)^{r-s} \binom{r}{s} C_{n+s(p-1)}^{(k)} \equiv 0 \pmod{p^{r+\nu(k)}},$$

it follows from the inductive hypothesis that

$$\frac{1}{k!} A_k \sum_{s=0}^{r} (-1)^{r-s} \binom{r}{s} C_{n+s(p-1)}^{(k)} \equiv 0 \pmod{p^r}$$

for all $k < h$. Hence (3.13) reduces to

$$\frac{1}{h!} A_h \sum_{s=0}^{r} (-1)^{r-s} \binom{r}{s} C_{n+s(p-1)}^{(h)} \equiv 0 \pmod{p^r}.$$

For $n = r + r_0$, $h = rp + r_0$, this becomes because of (3.12)

$$\frac{1}{h!} A_h C_h^{(h)} \equiv 0 \pmod{p^r}.$$

Since $C_h^{(h)} = h!$, we get

$$A_h \equiv 0 \pmod{p^r},$$

that is

$$A_h \equiv 0 \pmod{p^{[(h/p)]}}.$$

This completes the proof of (3.3).

We may now state

THEOREM 2. *Let*

$$f(x) = \sum_{n=0}^{\infty} a_n \frac{x^n}{n!} = \sum_{k=0}^{\infty} A_k \frac{(e^x-1)^k}{k!} \tag{3.14}$$

be an arbitrary series $\epsilon\,\mathfrak{H}$ *(or* $\mathfrak{H}_p$*). Then*

$$\sum_{s=0}^{r} (-1)^s \binom{r}{s} a_{n+s(p-1)} \equiv 0 \pmod{p^r} \tag{3.15}$$

for all $n \geqslant r \geqslant 0$ *if and only if*

$$A_k = 0 \pmod{p^{[k/p]}}$$

for all $k \geqslant 0$.

In particular, if the a_n are integral, then (3.15) is satisfied if and only if

$$f(x) = b_0 + \sum_{k=1}^{\infty} b_k \frac{(e^x-1)^k}{s_k},$$

where

$$s_k = \prod_{p \mid k} p^{\nu(k)} \tag{3.16}$$

and the b_k are integral.

4. We shall now suppose that in (3.14) $a_0 = A_0 = 0$. There is evidently no less in generality in making this assumption. We shall prove the following theorem which generalizes Theorem 1.

THEOREM 3. *Let*

$$f(x) = \sum_{n=1}^{\infty} a_n \frac{x^n}{n!} = \sum_{k=1}^{\infty} A_k \frac{(e^x-1)^k}{k!}, \tag{4.1}$$

where

$$A_k \equiv 0 \pmod{p^{[k/p]}}.$$

Put

$$f^k(x) = \sum_{n=k}^{\infty} a_n^{(k)} \frac{x^n}{n!}.$$

Then

$$\sum_{s=0}^{r} (-1)^s \binom{r}{s} a_{n+s(p-1)}^{(k)} \equiv 0 \pmod{p^{r+\nu(k)}} \qquad (n \geqslant r),$$

where $\nu(k)$ *is defined by* (2.4).

It will be convenient to first prove

THEOREM 4. *Let*

$$g(x) = \sum_{n=1}^{\infty} A_n \frac{x^n}{n!},$$

where the A_n *are integral* (mod p) *and*

(4.2) $$A_n \equiv 0 \pmod{p^{[n/p]}}.$$

Put

(4.3) $$g^k(x) = \sum_{n=k}^{\infty} A_n^{(k)} \frac{x^n}{n!} \qquad (k = 1, 2, 3, \ldots).$$

Then

(4.4) $$A_n^{(k)} \equiv 0 \pmod{p^{[n/p]+\nu(k)}}.$$

Proof. We have

$$g(x) = \sum_{j=0}^{p-1} \sum_{n=0}^{\infty} A_{pn+j} \frac{x^{pn+j}}{(pn+j)!} \qquad (A = 0).$$

By (4.2)

$$A_{pn+j} \equiv 0 \pmod{p^n},$$

so that

$$g(x) = \sum_{j=0}^{p-1} x^j g_j(x^p),$$

where

$$g_j(x) = \sum_{n=0}^{\infty} A_{pn+j} \frac{x^n}{(pn+j)!} \in \mathfrak{H} \text{ (or } \mathfrak{H}_p)$$

for $j = 0, 1, \ldots, p-1$. Expanding by the multinomial theorem we get

$$g^k(x) = \sum_{k_0+\cdots+k_{p-1}=k} \frac{k!}{k_0! \ldots k_{p-1}!} \big(g_0(x^p)\big)^{k_0} \big(x g_1(x^p)\big)^{k_1} \ldots \big(x^{p-1} g_{p-1}(x^p)\big)^{k_{p-1}}.$$

We seek the highest power of p dividing the term x^n on the right. The multinomial coefficient contributes

$$\mu(k) - \mu(k_0) - \ldots - \mu(k_{p-1}),$$

while

$$x^{k_1+2k_2+\cdots+(p-1)k_{p-1}}$$

contributes

$$\mu\big(k_1 + 2k_2 + \ldots + (p-1)k_{p-1}\big)$$

and $g_0^{k_0}$ contributes $\mu(k_0)$; in addition we have

$$\frac{n - \big(k_1 + 2k_2 + \ldots + (p-1)k_{p-1}\big)}{p}.$$

Thus it will suffice to show that

$$\mu(k) - \sum_{j=1}^{p-1} \mu(k_j) + \mu\Big(\sum_{j=1}^{p-1} jk_j\Big) + \frac{1}{p}\Big(n - \sum_{j=1}^{p-1} jk_j\Big) \geqslant \Big[\frac{n}{p}\Big] + \nu(k).$$

Since

$$\frac{1}{p}\Big(n - \sum_{j=1}^{p-1} jk_j\Big) = \Big[\frac{n}{p}\Big] - \Big[\frac{1}{p} \sum_{j=1}^{p-1} jk_j\Big],$$

this reduces to

$$\mu(k) - \sum_{j=1}^{p-1} \mu(k_j) + \mu\Big(\sum_{j=1}^{p-1} jk_j\Big) - \Big[\frac{1}{p} \sum_{j=1}^{p-1} jk_j\Big] \geqslant \nu(k),$$

which is the same as

(4.5) $$\Big[\frac{k}{p}\Big] + \nu\Big(\sum_{j=1}^{p-1} jk_j\Big) - \sum_{j=1}^{p-1} \nu(k_j) - \sum_{j=1}^{p-1} \Big[\frac{k_j}{p}\Big] \geqslant 0.$$

Since

$$\left[\frac{k}{p}\right] \geqslant \sum_{j=1}^{p-1}\left[\frac{k_j}{p}\right]$$

and

$$\nu\Big(\sum_{j=1}^{p-1} jk_j\Big) \geqslant \nu\Big(\sum_{j=1}^{p-1} k_j\Big) \geqslant \sum_{j=1}^{p-1} \nu(k_j),$$

(4.5) holds. We have therefore completed the proof of (4.4).

It is now easy to prove Theorem 3. By (4.1) and (4.3) we have

$$f^k(x) = \sum_{n=k}^{\infty} A_n^{(k)} \frac{(e^x-1)^n}{n!},$$

so that

$$(D^p-D)^r f^k(x) = \sum_{n=k}^{\infty} A_n^{(k)} (D^p-D)^r \frac{(e^x-1)^n}{n!}.$$

By (2.6)

$$(D^p-D)^r \frac{(e^x-1)^n}{n!} \equiv 0 \pmod{p^{r-[n/p]}} \qquad (r \geqslant [n/p]),$$

by (4.4) this becomes

$$(4.6) \qquad A_n^{(k)} (D^p-D)^r \frac{(e^x-1)^n}{n!} \equiv 0 \pmod{p^{r+\nu(k)}} \qquad (r \geqslant [n/p]).$$

For all r we have

$$A_n^{(k)} (D^p-D)^r \frac{(e^x-1)^n}{n!} \equiv 0 \pmod{p^{[n/p]+\nu(k)}},$$

so that (4.6) holds for $r < [n/p]$ also. Therefore

$$(D^p-D)^r f^k(x) \equiv 0 \pmod{p^{r+\nu(k)}}.$$

This completes the proof of Theorem 3.

5. If

$$(5.1) \qquad f(x) = \sum_{n=1}^{\infty} a_n \frac{x^n}{n!} \qquad (a_1 = 1),$$

where the a_n are integral (or integral $(\mathrm{mod}\,p)$), then the inverse of $f(x)$ is a series of the same kind;

$$\sum_{n=1}^{\infty} d_n \frac{x^n}{n!} \qquad (d_1 = 1),$$

where the d_n are integral (or integral $(\mathrm{mod}\,p)$). (The condition $a = d_1 = 1$ can be replaced by the weaker condition $a_1 d_1 = 1$, $a_1 \not\equiv 0 \pmod p$).

Thus if $g(x)$ is an arbitrary series in $\mathfrak{H}$ (or $\mathfrak{H}_p$) it follows that

$$(5.2) \qquad g(x) = \sum_{n=0}^{\infty} b_n \frac{x^n}{n!} = \sum_{k=0}^{\infty} A_k \frac{f^k(x)}{k!},$$

where the A_k are integral (or integral $(\mathrm{mod}\,p)$).

For brevity we let $\mathfrak{K}$ (or $\mathfrak{K}_p$) denote the set of series

$$\sum_{n=0}^{\infty} c_n \frac{x^n}{n!} \in \mathfrak{H} \text{ (or } \mathfrak{H}_p)$$

such that

$$\sum_{s=0}^{r} (-1)^s \binom{r}{s} c_{n+s(p-1)} \equiv 0 \pmod{p^r}$$

for all $n \geqslant r \geqslant 0$.

Suppose now that $f(x)$ as defined by (5.1) is a fixed series in $\mathfrak{K}$ (or $\mathfrak{K}_p$) and $g(x)$ is a series defined by (5.2). We seek necessary and sufficient conditions that $g(x) \in \mathfrak{K}$ (or $\mathfrak{K}_p$).

From (5.2) we get

$$(5.3) \qquad (D^p-D)^r g(x) = \sum_{k=1}^{\infty} A_k (D^p-D)^r \frac{f^k(x)}{k!}.$$

By Theorem 3

$$(D^p-D)^r f^k(x) \equiv 0 \pmod{p^{r+\nu(k)}},$$

so that

$$(D^p-D)^r \frac{f^k(x)}{k!} \equiv 0 \pmod{p^{r-[k/p]}} \qquad (r \geqslant [k/p]).$$

If we assume that the coefficients A_k occurring in (5.2) satisfy

$$(5.4) \qquad A_k \equiv 0 \pmod{p^{[k/p]}} \qquad (k = 1, 2, 3, \ldots),$$

it follows that

$$A_k(D^p-D)^r\frac{f^k(x)}{k!}\equiv 0\ (\mathrm{mod}\ p^r) \tag{5.5}$$

for $r \geqslant [k/p]$. Indeed it is evident from (5.4) that (5.5) holds for $r < [k/p]$ also.

Thus (5.3) implies

$$(D^p-D)^r g(x)\equiv 0\ (\mathrm{mod}\ p^r),$$

which is equivalent to

$$\sum_{s=0}^{r}(-1)^s\binom{r}{s}b_{n+s(p-1)}\equiv 0\ (\mathrm{mod}\ p^r)\qquad (n\geqslant r). \tag{5.6}$$

Therefore it follows from (5.4) that $g(x)\,\epsilon\,\mathfrak{K}$ (or $\mathfrak{K}_p$).

Conversely suppose that (5.6) holds for all $n \geqslant r \geqslant 0$. We shall show that this implies (5.4).

Assume that (5.4) holds for all $k<h$, and put

$$h = rp+r_0\qquad (0\leqslant r_0<p).$$

It is clear from (5.2) that

$$b_n=\sum_{k=0}^{N}\frac{1}{k!}A_k a_n^{(k)}\qquad (N\geqslant n), \tag{5.7}$$

where

$$f^k(x)=\sum_{n=k}^{\infty}a_n^{(k)}\frac{x^n}{n!}.$$

Note that

$$a_n^{(k)}=0\qquad (k>n). \tag{5.8}$$

From (5.7) we get

$$\sum_{s=0}^{r}(-1)^s\binom{r}{s}b_{n+s(p-1)}=\sum_{k=0}^{N}\frac{1}{k!}A_k\sum_{s=0}^{r}(-1)^s\binom{r}{s}a_{n+s(p-1)}^{(k)}$$

$$(N\geqslant n+r(p-1))$$

and therefore by (5.6)

$$\sum_{k=0}^{N}\frac{1}{k!}A_k\sum_{s=0}^{r}(-1)^s\binom{r}{s}a_{n+s(p-1)}^{(k)}\equiv 0\ (\mathrm{mod}\ p^r)\qquad (N\geqslant n+r(p-1)). \tag{5.9}$$

In (5.9) take $n=r+r_0$, $N=h$. Since by Theorem 3

$$\sum_{s=0}^{r}(-1)^s\binom{r}{s}a_{n+s(p-1)}^{(k)}\equiv 0\ (\mathrm{mod}\ p^{r+\nu(k)})\qquad (n\geqslant r),$$

it follows from the inductive hypothesis that

$$\frac{1}{k!}A_k\sum_{s=0}^{r}(-1)^s\binom{r}{s}a_{n+s(p-1)}^{(k)}\equiv 0\ (\mathrm{mod}\ p^r)$$

for all $k<h$. Hence (5.9) reduces to

$$\frac{1}{h!}A_h\sum_{s=0}^{r}(-1)^s\binom{r}{s}a_{n+s(p-1)}^{(k)}\equiv 0\ (\mathrm{mod}\ p^r).$$

For $n=r+r_0$, $h=rp+r_0$ this becomes because of (5.8)

$$\frac{1}{h!}A_h a_h^{(h)}\equiv 0\ (\mathrm{mod}\ p^r);$$

since $a_h^{(h)}=h!$ we get

$$A_h\equiv 0\ (\mathrm{mod}\ p^r),$$

that is

$$A_h\equiv 0\ (\mathrm{mod}\ p^{[h/p]}).$$

This completes the proof of (5.4).

We may now state

THEOREM 5. *Let $f(x)$ be a fixed series in $\mathfrak{K}$ (or $\mathfrak{K}_p$) of the form* (5.1). *Let $g(x)$ be an arbitrary series in $\mathfrak{H}$ (or $\mathfrak{H}_p$) and put*

$$g(x)=\sum_{k=0}^{\infty}A_k\frac{f^k(x)}{k!},$$

so that the A_k are necessarily integral (*or integral* (mod p)). *Then $g(x)\,\epsilon\,\mathfrak{K}$ (or $\mathfrak{K}$) if and only if*

$$A_k\equiv 0\ (\mathrm{mod}\ p^{[k/p]})$$

for all $k\geqslant 0$.

In particular (compare the remark immediately following Theorem 2), if the a_n are integral, then $g(x)\,\epsilon\,\mathfrak{K}$ if and only if

$$g(x)=b_0+\sum_{k=1}^{\infty}b_k\frac{f^k(x)}{s_k},$$

where s_k is defined by (3.16) and the b_k are integral.

6. Let

$$f(x) = \sum_{n=0}^{\infty} a_n \frac{x^n}{n!} \tag{6.1}$$

be an arbitrary series in $\mathfrak{H}$ (or $\mathfrak{H}_p$). It follows from (3.1), (3.2) and (3.11) that

$$a_n = \sum_{k=0}^{N} \frac{1}{k!} A_k \sum_{j=0}^{k} (-1)^{k-j} \binom{k}{j} j^n = \sum_{j=0}^{N} j^n \sum_{k=j}^{N} (-1)^{k-j} \binom{k}{j} \frac{A_k}{k!}$$

for arbitrary $N \geqslant n$. Thus we have

$$a_n = \sum_{j=0}^{N} j^n U_j^{(N)} \qquad (N \geqslant n), \tag{6.2}$$

where

$$U_j^{(N)} = \sum_{k=j}^{N} (-1)^{k-j} \binom{k}{j} \frac{A_k}{k!}. \tag{6.3}$$

We remark first that for given a_n, the numbers $U_j^{(N)}$ are uniquely determined by (6.2). Indeed for N fixed and $n = 0, 1, \ldots, N$, (6.2) is a system of $N+1$ equations in the $N+1$ unknowns $U_j^{(N)}$; the determinant of the system is

$$|j^n| \qquad (j, n = 0, 1, \ldots, N)$$

which is clearly not zero. Thus (6.3) furnishes the solution of the system (6.2).

In the next place we note that (6.3) implies

$$U_j^{(j)} = \frac{A_j}{j!} \tag{6.4}$$

and therefore (6.3) becomes

$$U_j^{(N)} = \sum_{k=j}^{N} (-1)^{k-j} \binom{k}{j} U_k^{(k)}. \tag{6.5}$$

By means of (6.5) all the $U_j^{(N)}$ are easily computed when the $U_k^{(k)}$ are known.

Nielsen ([3], Chapter 14) uses (6.2) in the case of integral $U_j^{(N)}$ to obtain Kummer's congruence for the a_n and thus obtains Kummer's congruence for the Euler Numbers. However it is by no means necessary

to assume that the $U_j^{(N)}$ are integral. Indeed by (6.4) and Theorem 2 we obtain the following criterion.

THEOREM 6. *Let*

$$f(x) = \sum_{n=0}^{\infty} a_n \frac{x^n}{n!}$$

be an arbitrary series in $\mathfrak{H}$ (*or* $\mathfrak{H}_p$) *and let* $U_j^{(N)}$ *be determined by* (6.2). *Then* $f(x) \in \mathfrak{K}$ (*or* $\mathfrak{K}_p$) *if and only if*

$$p^{\nu(k)} U_k^{(k)} \tag{6.6}$$

is integral (mod p).

References

[1] A. Hurwitz, *Über die Entwickelungskoefficienten der lemniskatischen Funktionen*, Mathematische Werke, vol. 2. pp. 342-373, Basel 1933.

[2] E. E. Kummer, *Über eine allgemeine Ergenschaft der rational Entwickelungs-koefficienten einer bestimmten Gattung analytischer Funktionen*, Journal für die reine und angewandte Mathematik 41 (1851), pp. 368-372.

[3] N. Nielsen, *Traité élémentaire des nombres de Bernoulli*, Paris 1923.

DUKE UNIVERSITY

Reçu par la Rédaction le 25. 6. 1960