SOME PROBLEMS CONCERNING KUMMER'S CONGRUENCES FOR THE EULER NUMBERS AND POLYNOMIALS

BY

L. CARLITZ AND JACK LEVINE

1. **Introduction.** The Euler polynomial $E_m(a)$ of degree m may be defined as the unique polynomial solution of the equation

$$E_m(a+1) + E_m(a) = 2a^m. \tag{1.1}$$

In particular, we have in the notation of Nörlund [3, Chapter 2]

$$C_m = 2^m E_m(0), \qquad E_m = 2^m E_m(1/2). \tag{1.2}$$

Let p be an odd prime, a and c fixed rational numbers that are integral (mod p); moreover $c \not\equiv 0 \pmod{p}$. Put

$$e_m = c^m E_m(a). \tag{1.3}$$

Then it is well known that the rational numbers e_m satisfy Kummer's congruence [2, Chapter 14]

$$\sum_{s=0}^{r} (-1)^s \binom{r}{s} e_{m+s(p-1)} \equiv 0 \pmod{(p^m, p^r)}, \tag{1.4}$$

where (p^m, p^r) denotes the greatest common divisor. Indeed more generally we have

$$\sum_{s=0}^{r} (-1)^s \binom{r}{s} e_{m+sw} \equiv 0 \pmod{(p^m, p^{rk})}, \tag{1.5}$$

provided $p^{k-1}(p-1) \mid w$. In particular the congruences (1.4) and (1.5) hold for the numbers C_m, E_m defined by (1.2).

It is natural to ask whether (1.4) is "best possible" in the following sense. To begin with, for $r=1$, what is the least positive integer μ such that

$$e_{m+\mu} \equiv e_m \pmod{p} \tag{1.6}$$

for all $m \geqq 1$? Secondly what is the least positive integer μ such that

$$\sum_{s=0}^{r} (-1)^s \binom{r}{s} e_{m+s\mu} \equiv 0 \pmod{(p^m, p^r)} \tag{1.7}$$

Presented to the Society November 21, 1959; received by the editors August 10, 1959.

for all m and fixed r? What is the least positive t such that

$$\sum_{s=0}^{t}(-1)^s\binom{t}{s}e_{m+s(p-1)} \equiv 0 \pmod{(p^m, p^r)} \tag{1.8}$$

for all m and fixed r? Similarly for (1.5) we seek (i) the least positive μ such that

$$e_{m+\mu} \equiv e_m \pmod{(p^m, p^k)} \tag{1.9}$$

for all m and fixed k; (ii) the least positive μ such that

$$\sum_{s=0}^{r}(-1)^s\binom{r}{s}e_{m+s\mu} \equiv 0 \pmod{(p^m, p^{rk})} \tag{1.10}$$

for all m, r and fixed k; (iii) the least positive t such that

$$\sum_{s=0}^{t}(-1)^s\binom{t}{s}e_{m+sw} \equiv 0 \pmod{(p^m, p^{rk})} \tag{1.11}$$

for all m and fixed r, k, where $w=p^{k-1}(p-1)$.

We shall show that for (1.6) and (1.7) $\mu=p-1$; for (1.8) we show that $t=r$ provided $2^p\not\equiv 2 \pmod{p^2}$ and $p\geqq 2r^2+1$. For (1.9) and (1.10) we show that $\mu=p^{k-1}(p-1)$ provided $p>3$; for (1.11) we show that $t=r$ provided $2^p\not\equiv 2 \pmod{p^2}$ and $p\geqq 2r^2+1$. It is then clear what is meant by saying that (1.4) is best possible; similarly for (1.5) with $w=p^{k-1}(p-1)$. While (1.6), (1.7), (1.8) are special cases of (1.9), (1.10), (1.11), respectively, it is convenient to treat separately the indicated cases.

We observe that in certain of the results enumerated above, the case of small p is left open. A special discussion of (4.3) below when $p=3$ suggests that some of the general results may indeed require modification for small values of p.

It should be observed that if m in (1.4) or (1.5) is restricted to an arithmetic progression, then the theorems of this paper no longer apply. For a special result of this nature see Theorem 9 below.

2. In order to show that μ in (1.6) is equal to $p-1$ we require the following preliminary result. Put

$$D_p = |e_{i+j+1}| \qquad (i, j = 0, 1, \cdots, p-2), \tag{2.1}$$

a determinant of order $p-1$. We shall show that

$$D_p \equiv \not\equiv 1 \pmod{p}. \tag{2.2}$$

Making use of the fact that

$$e_{m+p-1} \equiv e_m \pmod{p}$$

for $m\geqq 1$, it is easily verified that $D_p\equiv\not\equiv C_p \pmod{p}$, where C_p is the following circulant of order $p-1$:

$$C_p = \begin{vmatrix} e_1 & e_2 & e_3 \cdots e_{p-1} \\ e_{p-1} & e_1 & e_2 \cdots e_{p-2} \\ \cdots & \cdots & \cdots \\ e_2 & e_3 & e_4 \cdots e_1 \end{vmatrix}.$$

Now the familiar formula for the factorization of a circulant suggests the following analog:

$$C_p \equiv \prod_{r=1}^{p-1} \sum_{s=1}^{p-1} r^{s-1} e_s \pmod{p}. \tag{2.3}$$

Indeed, if (a_{r-s}) $(r, s = 1, \cdots, p-1)$ is an arbitrary circulant matrix of order $p-1$, then

$$(r^{s-1})(a_{r-s-1})(s^{1-r}) = (b_{rs}),$$

where

$$b_{rs} = \sum_{j=1}^{p-1} \sum_{k=1}^{p-1} r^{j-1} a_{j-k} s^{1-k} \equiv \sum_{i=0}^{p-2} \sum_{k=1}^{p-1} r^{i+k-1} a_i s^{1-k} \equiv \sum_{i=0}^{p-2} r^i a_i \sum_{k=0}^{p-2} (rs^{-1})^k \pmod{p}.$$

Since the inner sum $\equiv 0 \pmod{p}$ unless $r \equiv s \pmod{p}$, we get

$$b_{rs} \equiv -\delta_{rs} \sum_{i=0}^{p-2} r^i a_i.$$

Also

$$(r^{s-1})(s^{1-r}) = \left(\sum_{j=1}^{p-1} r^{j-1} s^{1-j} \right) \equiv (-\delta_{rs}).$$

Hence (2.3) follows at once.

In the next place, since

$$E_n(a + x) = \sum_{s=0}^{n} \binom{n}{s} x^{n-s} E_s(a),$$

we have

$$E_{p-1}(a - x) \equiv \sum_{s=0}^{p-1} x^{p-1-s} E_s(a) \pmod{p}.$$

Replacing x by r^{-1}, this becomes

$$E_{p-1}\left(a - \frac{1}{cr}\right) \equiv 1 + r \sum_{s=1}^{p-1} r^{s-1} c^s E_s(a) \equiv 1 + r \sum_{s=1}^{p-1} r^{s-1} e_s \pmod{p}. \tag{2.4}$$

Now it follows from (1.1) that

$$\sum_{s=1}^{n}(-1)^s s^k = \frac{1}{2}(-1)^n E_k(n+1) + \frac{1}{2}E_k(0). \tag{2.5}$$

For $k=p-1$, (2.5) becomes (since $E_{p-1}(0)=0$)

$$\sum_{s=1}^{n}(-1)^s \equiv \frac{1}{2}(-1)^n E_{p-1}(n+1) \pmod{p} \qquad (0 \leqq n < p).$$

Since

$$\sum_{s=1}^{n}(-1)^s = \begin{cases} -1 & (n \text{ odd}), \\ 0 & (n \text{ even}), \end{cases}$$

we get

$$E_{p-1}(m) \equiv \begin{cases} 2 & (m \text{ even}), \\ 0 & (m \text{ odd}), \end{cases} \qquad (1 \leqq m \leqq p). \tag{2.6}$$

Returning to (2.4), we define m by means of

$$m \equiv a - \frac{1}{cr} \pmod{p} \qquad (1 \leqq m \leqq p).$$

Then, using (2.6), it is clear that

$$r\sum_{s=1}^{p-1} r^{s-1}e_s \equiv \not\equiv 1 \pmod{p} \qquad (1 \leqq r \leqq p-1).$$

This yields

$$\prod_{r=1}^{p-1}\sum_{s=1}^{p-1} r^{s-1}e_s \equiv \not\equiv 1 \pmod{p}.$$

Substituting in (2.3), we get (2.2).

3. We now prove

THEOREM 1. *Assume that the numbers e_m defined by* (1.3) *satisfy the congruence*

$$e_{m+k} + c_1 e_{m+k-1} + \cdots + c_k e_m \equiv 0 \pmod{p}, \tag{3.1}$$

for all $m \geqq 1$, where $c_1, \cdots, c_k$ are integral (mod p) *and independent of m. Then $k \geqq p-1$.*

If we assume $k<p-1$, it follows from (3.1) that $D_p \equiv 0 \pmod{p}$. Since this contradicts (2.2), the theorem is proved.

As an immediate corollary of Theorem 1 we have

THEOREM 2. *The least positive integer μ such that*

$$e_{m+\mu} \equiv e_m \pmod{p}$$

for all $m \geqq 1$, *is* $\mu = p-1$.

Turning next to the congruence

$$\sum_{s=0}^{r} (-1)^s \binom{r}{s} e_{m+s\mu} \equiv 0 \pmod{(p^m, p^r)} \tag{3.2}$$

for all m and fixed r, we assume that μ is the smallest positive integer for which (3.2) holds. It follows that

$$\sum_{s=0}^{r} (-1)^s \binom{r}{s} e_{m+s\mu} \equiv 0 \pmod{p} \tag{3.3}$$

for all $m \geqq 1$.

The polynomials $(1-x^\mu)^r$ and $1-x^{p-1}$ have a greatest common divisor (mod p) of the form $1-x^d$, where $d \mid p-1$. Thus there exist polynomials $A(x)$, $B(x)$ with integral coefficients such that

$$(1 - x^\mu)^r A(x) + (1 - x^{p-1})B(x) \equiv 1 - x^d \pmod{p}.$$

Consequently we get (symbolically)

$$e^m(1 - e^\mu)^r A(e) + e^m(1 - e^{p-1})B(e) \equiv e^m(1 - e^d) \pmod{p}.$$

Using (3.3) and (1.4) this reduces to

$$e_{m+d} \equiv e_m \pmod{p}$$

for all $m \geqq 1$. In view of Theorem 2, $d = p-1$. Then

$$(1 - x^{p-1}) \mid (1 - x^\mu)^r \pmod{p},$$

which implies $\mu = p-1$. This completes the proof of

THEOREM 3. *The least positive integer* μ *such that*

$$\sum_{s=0}^{r} (-1)^s \binom{r}{s} e_{m+s\mu} \equiv 0 \pmod{(p^m, p^r)} \tag{3.4}$$

for all m *and fixed* r *is* $\mu = p-1$.

4. We consider next the congruence

$$\sum_{s=0}^{t} (-1)^s \binom{t}{s} e_{m+s(p-1)} \equiv 0 \pmod{(p^m, p^r)} \tag{4.1}$$

and seek the least positive integer t such that (4.1) holds for all m and fixed r. Clearly $1 \leqq t \leqq r$; also if (4.1) holds for a certain t it will hold for all larger t. Hence it will suffice to show that

$$\sum_{s=0}^{t} (-1)^s \binom{t}{s} e_{m+s(p-1)} \equiv 0 \pmod{(p^m, p^{t+1})} \tag{4.2}$$

for all m and any fixed $t \geqq 1$ is impossible.

We first examine the case $t=1$, namely the congruence

$$c_{m+p-1} \equiv e_m \pmod{p^2} \qquad (m \geqq 2). \tag{4.3}$$

Since, for all m, $E_m(a+p) \equiv E_m(a) + mpE_{m-1}(a) \pmod{p^2}$, it follows from (1.3) and (4.3) that

$$c^{p-1}E_{m+p-1}(a+p) - E_m(a+p) \equiv -pE_{m-1}(a) \pmod{p^2} \tag{4.4}$$

for $m \geqq 2$. Also (compare (2.5))

$$E_k(a+p) + E_k(a) = 2\sum_{s=0}^{p-1} (-1)^s (a+s)^k,$$

so that

$$\{c^{p-1}E_{m+p-1}(a-p) - E_m(a+p)\} + \{c^{p-1}E_{m+p-1}(a) - E_m(a)\}$$
$$= 2\sum_{s=0}^{p-1} (-1)^s (a+s)^m \{(a+s)^{p-1}c^{p-1} - 1\}.$$

Then, using (4.3) and (4.4), this reduces to

$$2\sum_{s=0}^{p-1} (-1)^s (a+s)^m \{(a+s)^{p-1}c^{p-1} - 1\} \equiv -pE_{m-1}(a) \pmod{p^2}, \tag{4.5}$$

for all $m \geqq 2$. It is convenient to replace m by $m+1$, so that (4.5) becomes

$$2\sum_{s=0}^{p-1} (-1)^s (a+s)^{m-1} \{(a+s)^{p-1}c^{p-1} - 1\} \equiv -pE_m(a) \pmod{p^2} \tag{4.6}$$

valid for all $m \geqq 1$. We now multiply both sides of (4.6) by $(a+j)^{p-1-m}$, where $1 \leqq m \leqq p-1$ and $0 \leqq j \leqq p-1$; the value $j=j_0$ such that $p \mid a+j$ is omitted. Since

$$\sum_{m=1}^{p-1} (a-j)^{p-1-m}(a+s)^m \equiv \begin{cases} -1 \pmod{p} & (j=s), \\ 0 \pmod{p} & (j \neq s), \end{cases}$$

we get

$$2(-1)^j (a+j)\{(a+j)^{p-1}c^{p-1} - 1\} \equiv p\sum_{m=1}^{p-1} (a+j)^{p-1-m}E_m(a) \pmod{p^2} \tag{4.7}$$

for all $j \neq j_0$ such that $0 \leqq j \leqq p-1$.

In the next place, since

$$E_{p-1}(a-x) \equiv \sum_{m=0}^{p-1} x^{p-1-m}E_m(a) \pmod{p},$$

it is clear that

$$\sum_{m=1}^{p-1}(a+j)^{p-1-m}E_m(a) \equiv E_{p-1}(-j) - (a+j)^{p-1} \equiv E_{p-1}(p-j) - 1 \equiv (-1)^{j-1} \pmod{p},$$

where at the last step we have used (2.6). Consequently (4.7) becomes

$$(a+j)^p c^p - (a+j)c \equiv -\frac{1}{2}pc \pmod{p^2} \tag{4.8}$$

for all $j \neq j_0$, $0 \leqq j \leqq p-1$.

If we sum (4.8) over j we get

$$\sum_{j=0}^{p-1}(a+j)^p c^p - (a+j_0)^p c^p - \sum_{j=0}^{p-1}(a+j)c + (a+j_0)c \equiv -\frac{1}{2}(p-1)c \pmod{p^2}. \tag{4.9}$$

If $B_n(x)$ is the Bernoulli polynomial of degree n, we have

$$\sum_{j=0}^{p-1}(a+j)^p = \frac{B_{p+1}(a+p) - B_{p+1}(a)}{p+1} \equiv pB_p(a) \pmod{p^2},$$

$$B_p(a) = \sum_{s=0}^{p}\binom{p}{s}B_s a^{p-s} = a^p + \sum_{s=1}^{p-2}\binom{p}{s}B_s a^{p-s} + pB_{p-1}a + B_p \equiv a^p - a \pmod{p},$$

since by the Staudt-Clausen theorem

$$pB_{p-1} \equiv -1 \pmod{p}.$$

Thus

$$\sum_{j=0}^{p-1}(a+j)^p \equiv 0 \pmod{p^2}$$

and (4.9) reduces to

$$-pac - \frac{1}{2}p(p-1)c + (a+j_0)c \equiv -\frac{1}{2}p(p-1)c \pmod{p^2},$$

which simplifies to

$$a + j_0 \equiv pa \pmod{p^2}. \tag{4.10}$$

If $j_0 \neq 0$ or $p-1$, allowable values for j in (4.8) are $j_0 \neq 1$. For $j = j_0 + 1$, (4.8) becomes

$$c^p - c \equiv \left(a - \frac{1}{2}\right)pc \pmod{p^2},$$

while for $j=j_0-1$ we get

$$c^p - c \equiv -\left(a - \frac{1}{2}\right) pc \pmod{p^2}.$$

Consequently $a \equiv \pmod{p}/2$; by (4.10) this implies

$$a \equiv \frac{1}{2} \pmod{p^2} \qquad (j_0 \not\equiv 0,\ p-1). \tag{4.11}$$

Also (4.10) yields

$$a \equiv 0 \pmod{p^2} \qquad (j_0 = 0), \tag{4.12}$$

$$a \equiv 1 \pmod{p^2} \qquad (j_0 = p-1). \tag{4.13}$$

When (4.11) holds we have

$$c^p \equiv c \pmod{p^2},$$

so that (4.8) reduces to

$$\left(\frac{1}{2}+j\right)^p - \left(\frac{1}{2}+j\right) \equiv -\frac{1}{2}p \pmod{p^2}. \tag{4.14}$$

Put $j=(p-1)/2+k$, so that (4.14) becomes

$$k^p - k \equiv 0 \pmod{p^2} \qquad \left(k = 1, \cdots, \frac{1}{2}(p-1)\right). \tag{4.15}$$

Now Brauer [1] has proved that for $p \geqq 5$, the smallest primitive root $g \pmod{p^2}$ is less than p. If this least primitive root $< p/2$, then (4.15) is clearly impossible; if $g > p/2$, then $p-g < p/2$ and belongs to an exponent $\pmod{p^2}$ that is a multiple of p, so that again (4.15) is contradicted.

In the next place, when (4.12) holds, (4.8) becomes

$$j^p c^p - jc \equiv -\frac{1}{2} pc \pmod{p^2}. \tag{4.16}$$

Let

$$j^p \equiv j + pm_j \pmod{p^2} \qquad (j = 1, \cdots, p-1).$$

Since (4.16) with $j=1$ gives

$$c^p \equiv c - \frac{1}{2} pc \pmod{p^2},$$

we have

$$j^p c^p \equiv jc + pcm_j - \frac{1}{2} pcj \pmod{p^2}.$$

Comparing this with (4.16) we get

$$m_j \equiv \frac{1}{2}(j-1) \pmod{p}, \tag{4.17}$$

so that

$$j^p \equiv j + \frac{1}{2}p(j-1) \pmod{p^2} \qquad (j = 1, \cdots, p-1). \tag{4.18}$$

It is easy to see that (4.18) is impossible for $p \geqq 5$. Indeed for $j=2$ we have

$$2^p \equiv 2 + \frac{1}{2}p \pmod{p^2}$$

and therefore

$$4^p \equiv 4 + 2p \pmod{p^2}.$$

On the other hand, for $j=4$, (4.18) is

$$4^p \equiv 4 + \frac{3}{2}p \pmod{p^2}.$$

In the third place since $E_m(1) = -E_m(0)$ for $m \geqq 1$, it is clear that (4.13) and (4.12) are equivalent cases. We have therefore proved the impossibility of (4.3) for all $p \geqq 5$. We may state

THEOREM 4 ($p>3$). *The congruence*

$$e_{m+p-1} \equiv e_m \pmod{p^2} \tag{4.19}$$

cannot hold for all $m \geqq 2$.

That the condition $p>3$ is necessary (for some values of a and c) can be seen as follows. Since

$$e_{m+4} - 2e_{m+2} + e_m \equiv 0 \pmod{9}$$

for all $m \geqq 2$, the assumption that

$$e_{m+2} \equiv e_m \pmod{9} \tag{4.20}$$

for some fixed $m = m_0 \geqq 2$ implies that (4.20) holds for all $m \geqq m_0$, $m \equiv m_0 \pmod{2}$.

In particular, since $E_2 = -1$, $E_4 = 5$,

$$E_4\left(\frac{1}{2}\right) \equiv E_2\left(\frac{1}{2}\right) \pmod{9}$$

and therefore

$$E_{m+2}\left(\frac{1}{2}\right) \equiv E_m\left(\frac{1}{2}\right) \pmod 9$$

for all $m \geqq 2$ (incidentally including odd values). Also $C_1 = -1$, $C_3 = 2$, $C_5 = -16$, we have

$$C_{m+2} \equiv C_m \pmod 9 \qquad (m \geqq 2).$$

5. We now return to (4.2). Since

$$E_m(a + p^t) \equiv E_m(a) + mp^t E_{m-1}(a) \pmod{p^{t+1}} \qquad (t \geqq 1),$$

it follows that

$$\sum_{s=0}^{t} (-1)^s \binom{t}{s} c^{m+s(p-1)} E_{m+s(p-1)}(a + p^t) \equiv \sum_{s=0}^{t} (-1)^s \binom{t}{s} e_{m+s(p-1)} \pmod{p^{t+1}},$$

since

$$\sum_{s=0}^{t} (-1)^s \binom{t}{s} (m + s(p-1)) c^{m+s(p-1)} E_{m+s(p-1)-1}(a) \equiv \sum_{s=0}^{t} (-1)^s \binom{t}{s} (m + s(p-1)) E_{m-1}(a) \equiv 0 \pmod p$$

for $t \geqq 2$ and $m \geqq 2$. Hence assuming that (4.2) holds we get

$$\sum_{s=0}^{t} (-1)^s \binom{t}{s} c^{m+s(p-1)} E_{m+s(p-1)}(a + p^t) \equiv 0 \pmod{p^{t+1}} \tag{5.1}$$

for $t \geqq 2$, $m \geqq t+1$. Since we have also

$$\sum_{j=0}^{p^t-1} (-1)^j (a + j)^m = \frac{1}{2} E_m(a + p^t) + \frac{1}{2} E_m(a),$$

(5.1) yields

$$\sum_{j=0}^{p^t-1} (-1)^j (a + j)^m c^m \left\{ (a + j)^{p-1} c^{p-1} - 1 \right\}^t \equiv 0 \pmod{p^{t+1}}.$$

It will be convenient to rewrite this as

$$\sum_{s=0}^{p^t-1} (-1)^s (a + s)^m \left\{ (a + s)^p c^p - (a + s)c \right\}^t \equiv 0 \pmod{p^{t+1}}, \tag{5.2}$$

which is asserted for $t \geqq 2$ and $m \geqq 1$. Now in the left member of (5.2) replace s by $j + pk$, where $0 \leqq j \leqq p-1$, $0 \leqq k \leqq p^{t-1} - 1$. Then (5.2) becomes

$$\sum_{j=0}^{p-1}(-1)^j\sum_{k=0}^{p^{t-1}-1}(-1)^k(a+j+pk)^m\{(a+j+pk)^pc^p-(a+j+pk)c\}^t \equiv 0 \pmod{p^{t+1}}. \tag{5.3}$$

Since

$$(a+j+pk)^p \equiv (a+j)^p \pmod{p^2},$$

the inner sum in (5.3)

$$\equiv (a+j)^m\sum_{k=0}^{p^{t-1}-1}(-1)^k\{(a+j)^pc^p-(a+j)c-pk\}^t$$

$$\equiv (a+j)^mp^t\sum_{k=0}^{p^{t-1}-1}(-1)^k(A_j-k)^t$$

$$\equiv (a+j)^mp^t\sum_{k=0}^{p^{t-1}-1}(-1)^k(A_j-p^{t-1}+1+k)^t$$

$$\equiv \frac{1}{2}(a+j)^mp^t\{E_t(A_j+1)+E_t(A_j+1-p^{t-1})\} \pmod{p^{t+1}},$$

where

$$A_j=\{(a+j)^pc^p-(a+j)c\}/p. \tag{5.4}$$

Since $t\geqq 2$, it is clear that

$$E_t(A_j+1-p^{t-1}) \equiv E_t(A_j+1) \pmod{p}.$$

Consequently (5.3) reduces to

$$\sum_{j=0}^{p-1}(-1)^j(a+j)^mE_t(A_j+1) \equiv 0 \pmod{p} \tag{5.5}$$

with A_j defined by (5.4). It then follows from (5.5) (compare the proof of (4.8)) that

$$E_t(A_j+1) \equiv 0 \pmod{p} \tag{5.6}$$

for all $j\neq j_0$, $0\leqq j<p$, where $a+j_0\equiv 0 \pmod{p}$.

It is clear from (5.6) that A_j can take on at most t distinct values (mod p). We shall show that for t fixed and p sufficiently large this is impossible—provided

$$2^p \not\equiv 2 \pmod{p^2}. \tag{5.7}$$

Put

$$N=[(p/2)^{1/2}], \tag{5.8}$$

where $[x]$ is the greatest integer $\leqq x$. Then, if (5.7) holds, at least N of the numbers

$$(a+j)^p c^p - (a+j)c \qquad (0 \leqq j < p, j \neq j_0) \tag{5.9}$$

are distinct (mod p^2). If we put $j=j_0+j'$ this is equivalent to the assertion that at least N of the numbers

$$j'^p c^p = j'c \qquad (-j_0 \leqq j' < p - j_0, j' \neq 0) \tag{5.10}$$

are distinct (mod p^2). If at most $N-1$ of the numbers (5.10) are distinct (mod p^2), then since $p-1 \geqq 2N^2$ it follows that, there exist at least $2N$ distinct numbers j_s' (mod p) such that

$$j_s'^p c^p - j_s' c \equiv kp \pmod{p^2} \qquad (s = 1, \cdots, 2N) \tag{5.11}$$

for some fixed k. Replacing j_s' by $p \neq j_s'$ we get a congruence of the same form with possibly a different k. Hence we may assume that (5.11) is satisfied by N values of j_s' such that $1 \leqq j_s' < p/2$. If we put

$$2^p \equiv 2 + wp \pmod{p^2} \qquad (p \neq w),$$

we get

$$(2j_s')^p c^p - 2j_s' c \equiv (2k + j_s' cw)p \pmod{p^2} \qquad (s = 1, \cdots, N).$$

These N numbers are distinct (mod p^2) so that we have a contradiction. Hence we have proved the assertion about (5.9). For the proof compare Vandiver [4].

It therefore follows that (5.6) is impossible when $N>t$, or, what is the same thing, when

$$p \geqq 2(t+1)^2 + 1. \tag{5.12}$$

We have now proved the impossibility of the congruence (4.2) subject to the condition (5.7) and (5.12). We may accordingly state the following

THEOREM 5. *The least positive integer t such that*

$$\sum_{s=0}^{t} (-1)^s \binom{t}{s} e_{m+s(p-1)} \equiv 0 \pmod{(p^m, p^r)}, \tag{5.13}$$

for all m and fixed $r \geqq 2$ is given by $t=r$ provided $2^p \not\equiv 2 \pmod{p^2}$ and

$$p \geqq 2r^2 + 1. \tag{5.14}$$

6. The symbolic identity

$$e^m(e^{p(p-1)} - 1) = \sum_{r=1}^{p} \binom{p}{r} e^m(e^{p-1} - 1)^r,$$

where after expansion e^n is replaced by e_n, evidently implies (for $m \geqq 3$)

$$e^m(e^{p(p-1)} - 1) \equiv pe^m(e^{p-1} - 1) \pmod{p^3}. \tag{6.1}$$

Thus the impossibility of (4.3) for $p>3$ implies that

$$e_{m+p(p-1)} - e_m \equiv 0 \pmod{p^3} \tag{6.2}$$

for all $m \geqq 3$ is impossible for $p > 3$.

Much more can be obtained in this way. In the identity

$$x^p - 1 = \sum_{s=1}^{p} \binom{p}{s} (x-1)^s \tag{6.3}$$

replace x by $e^{p^{k-1}(p-1)}$, so that

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

This yields

$$e^m(e^{p^k(p-1)} - 1) \equiv pe^m(e^{p^{k-1}(p-1)} - 1) \pmod{p^{k+2}} \tag{6.4}$$

for all $m \geqq k+2$. The case $k=1$ is that just discussed. For $k=2$ we have

$$e^m(e^{p^2(p-1)} - 1) \equiv pe^m(e^{p(p-1)} - 1) \pmod{p^4}.$$

We infer that

$$e^m(e^{p^2(p-1)} - 1) \equiv 0 \pmod{p^4}$$

for all $m \geqq 4$ is impossible ($p > 3$). Generally, by means of (6.4), an easy induction shows that

$$e^m(e^{p^{k-1}(p-1)} - 1) \equiv 0 \pmod{p^{k+1}} \tag{6.5}$$

for all $m \geqq k+1$ is impossible when $p > 3$.

In the congruence

$$e_{m+\mu} \equiv e_m \pmod{(p^m, p^k)}, \tag{6.6}$$

it is clear from Theorem 2 that $p-1 \mid \mu$. Therefore, applying the result obtained for (6.5), we may state

THEOREM 6 ($p > 3$). *The least positive integer μ such that* (6.6) *holds for all m and fixed $k \geqq 1$ is given by*

$$\mu = p^{k-1}(p-1). \tag{6.7}$$

Turning next to the congruence

$$\sum_{s=0}^{r} (-1)^s \binom{r}{s} e_{m+s\mu} \equiv 0 \pmod{(p^m, p^{rk})}, \tag{6.8}$$

which is assumed to hold for all m and fixed r, k, it is first of all easy to see that $p-1 \mid \mu$. Indeed, for $m \geqq 1$, (6.8) obviously implies

$$e^m(e^{\mu'} - 1)^r \equiv 0 \pmod{p^r}$$

with minimum $\mu' = p-1$; since

$$(x^{p-1}-1)^r \mid (x^\mu - 1)^r \pmod p$$

if and only if $p-1 \mid \mu$, the assertion above follows at once.

If we next raise both sides of (6.3) to the rth power we get an identity of the following kind:

$$\begin{aligned}(x^p-1)^r &= \{p(x-1)f(x-1) + (x-1)^p\}^r \\ &= p^r(x-1)^r f^r(x-1) + \cdots + (x-1)^{pr}.\end{aligned}$$

where $f(x-1)$ is a polynomial with integral coefficients. Now replacing x by $e^{p^{k-1}(p-1)}-1$, we get

$$e^m(e^{p^k(p-1)}-1)^r \equiv p^r e^m(e^{p^{k-1}(p-1)}-1)^r \pmod{p^{kr+r+1}} \tag{6.9}$$

for all $m \geqq kr+r+1$. An induction with respect to k yields the following

THEOREM 7 ($p>3$). *The least positive integer μ such that* (6.8) *holds for all m and fixed $k \geqq 1$, $r \geqq 1$ is given by* (6.7).

Finally we consider the congruence

$$\sum_{s=0}^{t} (-1)^s \binom{t}{s} e_{m+sw} \equiv 0 \pmod{(p^m, p^{rk})}, \tag{6.10}$$

where $w = p^{k-1}(p-1)$, for fixed r, k. Clearly we have $t \leqq r$. It will suffice to show that (6.10) is impossible when $t = r-1$. For, assuming that (6.10) holds when $t = r-1$, we get by repeated application of (6.9)

$$\begin{aligned}e^m(e^{p^{k-1}(p-1)}-1)^{r-1} &\equiv p^{r-1}e^m(e^{p^{k-2}(p-1)}-1)^{r-1} \\ &\equiv \cdots \equiv p^{(k-1)(r-1)}e^m(e^{p-1}-1)^{r-1} \pmod{p^{k(r-1)+1}}\end{aligned}$$

for $m \geqq kt-k$. Since by Theorem 4

$$e^m(e^{p-1}-1)^{r-1} \not\equiv 0 \pmod{p^r}$$

when certain conditions are satisfied, it follows that

$$e^m(e^{p^{k-1}(p-1)}-1)^{r-1} \not\equiv 0 \pmod{p^{k(r-1)+1}}$$

for all $m \geqq k(r-1)+1$. This completes the proof of

THEOREM 8. *The least positive integer t for which the congruence* (6.10) *is satisfied for all m and fixed $r \geqq 1$, $k \geqq 1$, is given by $t = r$, provided* $2^p \not\equiv 2 \pmod{p^2}$ *and*

$$p \geqq 2r^2 + 1.$$

7. As remarked in the Introduction, if m in (1.4) or (1.5) is restricted to an arithmetic progression, the theorems of this paper may not hold. We shall illustrate in a special case. It is clear, to begin with, that if

$$e_{m_0+p-1} \equiv e_{m_0} \pmod{p^2},$$

where m_0 is a fixed number $\geqq 2$, then it follows by repeated application of the congruence

$$e_{m+2p-2} - 2e_{m+p-1} + e_m \equiv 0 \pmod{p^2} \qquad (m \geqq 2)$$

that

$$e_{m+p-1} \equiv e_m \pmod{p^2}$$

for $m \equiv m_0 \pmod{p-1}$, $m \geqq m_0$.

In particular, since

$$E_{p+1} \equiv E_2 \equiv -1 \pmod{p},$$

we can determine an integer c such that

$$c^{p-1}E_{p+1} \equiv -1 \pmod{p^2}. \tag{7.1}$$

Hence, if we put

$$e_m = c^m E_m, \tag{7.2}$$

we have

$$e_{p+1} \equiv e_2 \pmod{p^2}$$

from which it follows that

$$e_{m+p-1} \equiv e_m \pmod{p^2} \tag{7.3}$$

for all

$$m \equiv 2 \pmod{p-1}, \qquad m \geqq 2. \tag{7.4}$$

This proves

THEOREM 9. *The numbers e_m defined by* (7.1) *and* (7.2) *satisfy* (7.3) *for all m in the arithmetic progression* (7.4).

REFERENCES

1. A. Brauer, *Elementary estimates for the least primitive root*, Studies in Mathematics and Mechanics presented to Richard von Mises, New York, 1954, pp. 20–29.

2. N. Nielsen, *Traité élémentaire des nombres de Bernoulli*, Paris, 1923.

3. N. E. Nörlund, *Vorlesungen über Differenzenrechnung*, Berlin, 1924.

4. H. S. Vandiver, *An aspect of the linear congruence with applications to the theory of Fermat's quotient*, Bull. Amer. Math. Soc. vol. 22 (1916) pp. 61–67.

DUKE UNIVERSITY,
DURHAM, NORTH CAROLINA
STATE COLLEGE OF AGRICULTURE AND ENGINEERING,
RALEIGH, NORTH CAROLINA