A NOTE ON EULER NUMBERS AND POLYNOMIALS

L. CARLITZ

1. Euler numbers. Let E_m denote the Euler number in the even suffix notation so that

$$(1.1)\qquad (E+1)^m+(E-1)^m=0 \quad (m>0), \quad E_0=1,$$

where, as usual, after expansion of the left member E^r is replaced by E_r. Nielsen [4, p. 273] has proved that

$$(1.2)\qquad E_{2m} \equiv \begin{cases} 0 \pmod{p} & (p \equiv 1 \pmod{4}) \\ 2 \pmod{p} & (p \equiv 3 \pmod{4}), \end{cases}$$

where p is an odd prime such that $p-1 \mid 2m$. The special case $m=p-1$ is due to Ely [1, p, 341].

We wish to point out, to begin with, that (1.2) can be extended to give

$$(1.3)\qquad E_{2m} \equiv \begin{cases} 0 \pmod{p^e} & (p \equiv 1 \pmod{4}) \\ 2 \pmod{p^e} & (p \equiv 3 \pmod{4}), \end{cases}$$

where p is an odd prime such that $(p-1)p^{e-1} \mid 2m$.

To prove (1.3) we begin with the formula

$$(1.4)\qquad E_m(x+1)+E_m(x)=2x^m,$$

where [5, p. 25]

$$(1.5)\qquad E_m(x)=\sum_{0 \leqq 2s \leqq m} \binom{m}{2s} 2^{-2s} \left(x-\frac{1}{2}\right)^{m-2s} E_{2s},$$

is the Euler polynomial of degree m. It is clear from (1.4) that

$$(1.6)\qquad 2\sum_{s=0}^{r}(-1)^s(x+s)^m = E_m(x)+(-1)^r E_m(x+r+1).$$

We also recall that [5, p. 28]

Received Feb. 18, 1954.

$$(1.7) \qquad E_m(x) = \sum_{s=0}^{m} \binom{m}{s} 2^{-s} C_s x^{m-s},$$

where

$$(1.8) \qquad C_{m-1} = 2^m(1-2^m)\frac{B_m}{m}; \quad C_0 = 1, \quad C_{2r} = 0 \qquad (r \geqq 1).$$

Consequently for $x = 0$, (1.5) and (1.6) imply

$$(1.9) \qquad 2\sum_{s=1}^{r}(-1)^{r-s}s^{2m} = E_{2m}(r+1) = 2^{-2m}\sum_{s=0}^{m}\binom{2m}{2s}(2r+1)^{2m-2s}E_{2s}.$$

Clearly (1.9) yields the congruence

$$(1.10) \qquad 2^{2m+1}\sum_{s=1}^{r}(-1)^{r-s}s^{2m} \equiv E_{2m} \qquad (\mathrm{mod}\ (2r+1)^2).$$

Now let $(p-1)p^{e-1} | 2m$ and $p^e | (2r+1)^2$. Then for $p \nmid s$ it is evident that $s^{2m} \equiv 1 \pmod{p^e}$, while for $p | s$ we have $s^{2m} \equiv 0 \pmod{p^e}$. Thus the left member of (1.10) is congruent to

$$(1.11) \qquad 2\sum_{\substack{s=1 \\ p \nmid s}}^{r}(-1)^{r-s} \qquad (\mathrm{mod}\ p^e).$$

Since $p | 2r+1$ implies $r \equiv \frac{1}{2}(p-1) \pmod{p}$, it follows at once that (1.11) reduces to

$$(1.12) \qquad 2(1-1+\ldots+(-1)^{\frac{1}{2}(p-3)}) = \begin{cases} 0 & (p \equiv 1 \pmod{4}) \\ 2 & (p \equiv 3 \pmod{4}). \end{cases}$$

Comparison of (1.10) and (1.12) leads at once to (1.3). This proves

THEOREM 1. *If* $(p-1)p^{e-1} | 2m$ *then* (1.3) *holds.*

For a different proof of (1.3) see [2, p. 845].

2. Euler polynomials. Returning to (1.6) we put $x = a$, where a is a rational umber that is integral $(\mathrm{mod}\ p)$. Since for $a \equiv b \pmod{p^e}$ we have $E_m(a) \equiv E_m(b) \pmod{p^e}$, there is no loss in generality in assuming that a is an integer.

If we take $r = p-1$, (1.6) becomes

$$(2.1) \qquad 2\sum_{s=0}^{p-1}(-1)^s(a+s)^{2m} = E_{2m}(a) + E_{2m}(a+p).$$

Let $a \equiv 0 \pmod{p}$ and assume that $(p-1)p^{e-1} | 2m$. Then (2.1) reduces to

$$E_{2m}(a) + E_{2m}(a+p) \equiv 0 \pmod{p^e}. \tag{2.2}$$

Since by (1.7) and (1.8), $E_{2m}(0) = 0$ for $m \geqq 1$ we therefore get from (2.2)

$$E_{2m}(a) \equiv 0 \pmod{p^e} \qquad (p | a). \tag{2.3}$$

For $a \equiv 1 \pmod{p}$ it is also clear that the left member of (2.1) is divisible by p^e; since $E_{2m}(1) = 0$ for $m \geqq 1$ we get

$$E_{2m}(a) \equiv 0 \pmod{p^e} \qquad (a \equiv 1 \pmod{p})). \tag{2.4}$$

In the next place, since

$$E_m(x+r) = \sum_{s=0}^{m} \binom{m}{s} r^{m-s} E_s(x),$$

it follows from (1.6) that

$$\begin{aligned} 2\sum_{s=0}^{r-1}(-1)^s(a+s)^{2m} &= (1+(-1)^{r-1})E_{2m}(a) + (-1)^{r-1}\sum_{s=0}^{2m-1}\binom{2m}{s} r^{2m-s}E_s(a) \\ &\equiv (1+(-1)^{r-1})E_{2m}(a) \pmod{r}. \end{aligned} \tag{2.5}$$

We take r odd, $p^e | r$ and $(p-1)p^{e-1} | 2m$; since

$$(a+p)^{2m} \equiv a^{2m} \pmod{p^e},$$

it follows at once from (2.5) that

$$E_{2m}(a+p) \equiv E_{2m}(a) \pmod{p^e}, \tag{2.6}$$

where a is arbitrary (but integral $\pmod{p}$).

Thus to determine the residue of $E_{2m}(a)$ it suffices to take $1 \leqq a \leqq p-1$. Using (1.6) we have

$$2\sum_{s=0}^{r}(-1)^{r-s}(a+s)^{2m} = (-1)^r E_{2m}(a) + E_{2m}(a+r+1),$$

which implies

$$2\sum_{s=0}^{r}(-1)^{r-s}(a+s)^{2m} \equiv (-1)^r E_{2m}(a) + 2^{-2m}E_{2m} \pmod{(2a+2r+1)^2}. \tag{2.7}$$

If we assume that $(p-1)p^{e-1} | 2m$ and $p^e | (2a+2r+1)^2$ then (2.7) becomes

$$(2.8) \qquad 2\sum_{\substack{s=0\\ p\nmid a+s}}^{r}(-1)^{r-s} \equiv (-1)^r E_{2m}(a) + E_{2m} \qquad (\operatorname{mod} p^e).$$

Clearly the left member of (2.8) is equal to

$$(2.9) \qquad 2\sum_{\substack{s=1\\ p\nmid s}}^{a+r}(-1)^{a+r-s} - 2\sum_{s=1}^{a-1}(-1)^{a+r-s}.$$

Comparing the first sum in (2.9) with (1.11) and using (1.3) it is clear that (2.8) becomes

$$(-1)^r E_{2m}(a) \equiv -2\sum_{s=1}^{a-1}(-1)^{a+r-s}$$

and therefore finally

$$(2.10) \qquad E_{2m}(a) \equiv 1 + (-1)^a \quad (\operatorname{mod} p^e) \qquad (1 \leqq a \leqq p-1).$$

We may state

THEOREM 2. *If* $(p-1)p^{e-1} | 2m$ *and* $p \nmid a$ *then*

$$(2.11) \qquad E_{2m}(a) \equiv 1 + (-1)^c \qquad (\operatorname{mod} p^e),$$

where $a \equiv c \pmod p$, $1 \leqq c \leqq p-1$; *if* $p | a$, *then* (2.3) *holds.*

It is evident that (2.11) includes (2.4); also it is not difficult to show that (2.11) includes (1.3).

3. Additional results. If in (1.6) we replace m by $2m-1$ we get using (1.5)

$$(3.1) \qquad 2\sum_{s=0}^{r}(-1)^s(a+s)^{2m-1} \equiv E_{2m-1}(a) \qquad (\operatorname{mod} 2a+2r+1).$$

Hence if $(p-1)p^{e-1} | 2m$ and $p^e | 2a+2r+1$, (3.1) implies

$$(3.2) \qquad 2\sum_{\substack{s=0\\ p\nmid a+s}}^{r}\frac{(-1)^s}{a+s} \equiv E_{2m-1}(a) \qquad (\operatorname{mod} p^e).$$

In particular when $a=0$, it follows from (1.8) that

$$(3.3) \qquad \sum_{\substack{s=0\\ p\nmid s}}^{\frac{1}{2}(p^e-1)}\frac{(-1)^s}{s} \equiv C_{2m-1} \equiv (1-2^{2m})\frac{B_{2m}}{2m} \qquad (\operatorname{mod} p^e);$$

the special case

https://doi.org/10.1017/S0027763000018043 Published online by Cambridge University Press

(3.4) $$\sum_{s=0}^{\frac{1}{2}(p-1)} \frac{(-1)^s}{s} \equiv C_{2m-1} \pmod{p} \qquad (p-1 \mid 2m)$$

may be noted. We also remark that for $a = \frac{1}{2}$, (3.2) becomes

(3.5) $$\sum_{\substack{s=0 \\ p \nmid 2s+1}}^{p^e} \frac{(-1)^s}{2s+1} \equiv 0 \pmod{p^e}.$$

For formulas like (3.4) see Glaisher [3].

If (a/p) denotes the Legendre symbol, then

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

Thus (1.6) implies

(3.6) $$2\sum_{s=0}^{r-1}(-1)^s\left(\frac{a+s}{p}\right) \equiv E_m(a) + (-1)^{r-1}E_m(a+r) \pmod{p^e},$$

where m is an odd multiple of $\frac{1}{2}(p-1)p^{e-1}$. Now let r be odd, $p^e \mid r$; then (3.6) yields

(3.7) $$\sum_{s=0}^{r-1}(-1)^s\left(\frac{a+s}{p}\right) \equiv E_m(a) \pmod{p^e}.$$

It follows at once from (3.7) that

(3.8) $$E_m(a+p) \equiv E_m(a) \pmod{p^e}.$$

Moreover it is clear from (3.7) that $(r = pt)$

$$\begin{aligned} E_m(a) &\equiv \sum_{j=0}^{t-1}\sum_{i=0}^{p-1}(-1)^{i+pj}\left(\frac{a+i}{p}\right) \\ &\equiv \sum_{j=0}^{t-1}(-1)^j\sum_{i=0}^{p-1}(-1)^i\left(\frac{a+i}{p}\right) \equiv \sum_{i=0}^{p-1}(-1)^i\left(\frac{a+i}{p}\right), \end{aligned}$$

so that

(3.9) $$E_m(a) \equiv \sum_{i=0}^{p-1}(-1)^i\left(\frac{a+i}{p}\right) \pmod{p^e}.$$

In particular for $a = 0$, (3.9) becomes

(3.10) $$E_m(0) \equiv \sum_{i=0}^{p-1}(-1)^i\left(\frac{i}{p}\right) \pmod{p^e}.$$

For $p \equiv 1 \pmod 4$, both members of (3.10) vanish, while for $p \equiv 3 \pmod 4$

https://doi.org/10.1017/S0027763000018043 Published online by Cambridge University Press

we get

$$C_m \equiv 2 \sum_{s=0}^{\frac{1}{2}(p-1)} (-1)^s \left(\frac{2s}{p}\right) \pmod{p^e}. \tag{3.11}$$

Let $1 \leqq a \leqq p-1$; then by (3.9)

$$\begin{aligned} E_m(a) &\equiv (-1)^a \sum_{s=a}^{p+a-1} (-1)^s \left(\frac{s}{p}\right) \\ &\equiv (-1)^a \sum_{s=0}^{p-1} (-1)^s \left(\frac{s}{p}\right) - 2(-1)^a \sum_{s=0}^{a-1} (-1)^s \left(\frac{s}{p}\right). \end{aligned}$$

Comparing with (3.10) we get

$$E_m(0) - E_m(a) \equiv 2(-1)^a \sum_{s=0}^{a-1} (-1)^s \left(\frac{s}{p}\right) \pmod{p^e}. \tag{3.12}$$

We may state

THEOREM 3. *If m is an odd multiple of $\frac{1}{2}(p-1)p^{e-1}$, then* (3.8), (3.10) *and* (3.12) *hold.*

In particular, (3.12) implies

$$C_m - E_m \equiv 2(-1)^{\frac{1}{2}(p+1)} \sum_{s=0}^{\frac{1}{2}(p-1)} (-1)^s \left(\frac{2s}{p}\right) \pmod{p^e}, \tag{3.13}$$

which includes (3.11).

4. Eulerian numbers and polynomials. It is of interest to compare (2.3) with the following known results for Bernoulli polynomials.

$$B_m(a) \equiv 0 \pmod{p^e} \qquad (p^e \mid m,\ p-1 \nmid m), \tag{4.1}$$

$$B_m(a) + \frac{1}{p} - 1 \equiv 0 \pmod{p^e} \qquad ((p-1)p^e \mid m), \tag{4.2}$$

where the rational number a is integral $(\mathrm{mod}\ p)$. However it seems more instructive to discuss the "Eulerian" numbers $\phi_m(\zeta)$ defined by

$$\frac{1-\zeta}{e^t-\zeta} = \sum_{m=0}^{\infty} \phi_m(\zeta) \frac{t^m}{m!} \qquad (\zeta \neq 1), \tag{4.3}$$

and the polynomials

$$\phi_m(x, \zeta) = \sum_{s=0}^{m} \binom{m}{s} x^{m-s} \phi_s(\zeta) = (x + \phi(\zeta))^m. \tag{4.4}$$

For a detailed study of $\phi_m(\zeta)$ see [2]. We shall suppose that the parameter ζ

https://doi.org/10.1017/S0027763000018043 Published online by Cambridge University Press

is an l-th root of unity, where $l \geqq 2$.

It is an immediate consequence of (4.4) that

$$\phi_m(x+1, \zeta) - \zeta\phi_m(x, \zeta) = (1-\zeta)x^m. \tag{4.5}$$

(Since $\phi_m(x, -1) = E_m(x)$, it is clear that (4.5) reduces to (1.4) when $\zeta = -1$). By means of (4.5) we readily obtain

$$\phi_m(x+r, \zeta) - \zeta^r \phi_m(x, \zeta) = (1-\zeta)\sum_{s=0}^{r-1}\zeta^{r-1-s}(x+s)^m. \tag{4.6}$$

Substituting from (4.4) it is evident that (4.6) implies

$$(1-\zeta^r)\phi_m(x, \zeta) + \sum_{s=1}^{m-1}\binom{m}{s} r^{m-s}\phi_m(x, \zeta) = (1-\zeta)\sum_{s=0}^{r-1}\zeta^{r-1-s}(x+s)^m. \tag{4.7}$$

Now replace x by a rational number a that is integral (mod p). The number $\phi_m(\zeta)$ is in the field $R(\zeta)$, where R is the rational field; more precisely it is of the form $\alpha_m/(1-\zeta)^m$, where α_m is an integer of $R(\zeta)$. If we assume that $(p, 1-\zeta) = (1)$, then $\phi_m(\zeta)$ is integral (mod p); the same is therefore true of $\phi_m(a, \zeta)$. In the next place (4.7) implies

$$(1-\zeta^r)\phi_m(x, \zeta) \equiv (1-\zeta)\sum_{s=0}^{r-1}\zeta^{r-1-s}(x+s)^m \pmod{r}, \tag{4.8}$$

provided $(r, 1-\zeta) = (1)$. Let us now assume that $(p-1)p^{e-1} \mid m$ and $p^e \mid r$. Then (4.8) reduces to

$$(1-\zeta^r)\phi_m(a, \zeta) \equiv (1-\zeta)\sum_{\substack{s=0 \\ p \nmid a+s}}^{r-1} \zeta^{r-1-s} \pmod{p^e}. \tag{4.9}$$

If we suppose, as we may, that $l \nmid r$, then it follows readily from (4.9) that

$$\phi_m(a+p, \zeta) \equiv \phi_m(a, \zeta) \pmod{p^e}. \tag{4.10}$$

It accordingly suffices to assume that $0 \leqq a \leqq p-1$.

In the first place for $a=0$, (4.9) reduces to

$$(1-\zeta^r)\phi_m(\zeta) \equiv (1-\zeta)\sum_{\substack{s=0 \\ p \nmid s}}^{r-1}\zeta^{r-1-s} \pmod{p^e}. \tag{4.11}$$

We shall take $r \equiv 1 \pmod{l}$; then (4.11) gives

https://doi.org/10.1017/S0027763000018043 Published online by Cambridge University Press

$$\phi_m(\zeta) \equiv \sum_{s=0}^{r-1} \zeta^{r-1-s} - \sum_{s=0}^{t-1} \zeta^{r-1-ps},$$

where $r = tp$. A little computation now gives

$$\phi_m(\zeta) = \frac{1-\zeta^{p-1}}{1-\zeta^p} \pmod{p^e}. \tag{4.12}$$

Next for $1 \leqq a \leqq p-1$, where again $r \equiv 1 \pmod{l}$, $r = tp$, it follows from (4.9) that

$$\begin{aligned} \phi_m(a, \zeta) &\equiv \sum_{s=0}^{a+r-1} \zeta^{a+r-1-s} - \sum_{s=0}^{a-1} \zeta^{a+r-1-s} - \sum_{s=1}^{t} \zeta^{a+r-1-ps} \\ &\equiv \frac{1-\zeta^{a+r}}{1-\zeta} - \zeta^r \frac{1-\zeta^a}{1-\zeta} - \zeta^{a-1} \frac{1-\zeta^{pt}}{1-\zeta^p} \\ &\equiv 1 - \zeta^{a-1} \frac{1-\zeta}{1-\zeta^p}. \end{aligned}$$

Hence using (4.10) we get

$$\phi_m(a, \zeta) \equiv 1 - \zeta^{c-1} \frac{1-\zeta}{1-\zeta^p} \pmod{p^e}, \tag{4.13}$$

where $a \equiv c \pmod{p}$, $1 \leqq c \leqq p-1$. This completes the proof of

THEOREM 4. *Let $(p-1)p^{e-1} \mid m$ and let $a \equiv c \pmod{p}$, where $0 \leqq c \leqq p-1$. Then if $c \neq 0$, (4.13) holds, while for $c = 0$ we have*

$$\phi_m(a, \zeta) \equiv \frac{1-\zeta^{p-1}}{1-\zeta^p} \pmod{p^e} \qquad (p \mid a). \tag{4.14}$$

It is clear that for $\zeta = -1$, (4.13) reduces to (2.11) and (4.14) reduces to (2.3). For the special case $a = 0$ of (4.14) see [2, p. 842].

If α is an integer of $R(\zeta)$, we may again employ (4.8). Let $\mathfrak{p}$ be a prime ideal of $R(\zeta)$, $N\mathfrak{p} = p^f$, where $(p, l) = 1$. Then if we assume that

$$(N\mathfrak{p} - 1)p^{e-1} \mid m, \tag{4.15}$$

and $p^e \mid r$, we get

$$(1-\zeta^r)\phi_m(\alpha, \zeta) \equiv (1-\zeta) \sum_{\substack{s=0 \\ \mathfrak{p} \nmid \alpha+s}}^{r-1} \zeta^{r-1-s} \pmod{\mathfrak{p}^e}. \tag{4.16}$$

It follows that if $\pi \in \mathfrak{p}$ then

$$\phi_m(\alpha + \pi, \zeta) \equiv \phi_m(\alpha, \zeta) \pmod{\mathfrak{p}^e}, \tag{4.17}$$

and therefore

(4.18) $$\phi_m(\alpha+p,\ \zeta)\equiv\phi_m(\alpha,\ \zeta)\qquad(\text{mod } p^e).$$

Now if α is congruent to a rational integer (mod $\mathfrak{p}$), then, in view of (4.17), (4.13) holds. On the other hand, when α is not congruent to a rational integer, then in the right member of (4.16) the condition $\mathfrak{p}\nmid\alpha+s$ is satisfied automatically and we get ($r\equiv 1$ (mod l))

$$\phi_m(a,\ \zeta)\equiv\sum_{s=0}^{r-1}\zeta^s\equiv\frac{1-\zeta^r}{1-\zeta}\equiv 1\qquad(\text{mod } \mathfrak{p}^e).$$

We may state

THEOREM 5. *Let α be an integer of $R(\zeta)$, $p\nmid l$, and assume that* (4.15) *is satisfied, where $\mathfrak{p}$ is a prime ideal of $R(\zeta)$, $N\mathfrak{p}=p^f$. Then if α is congruent to a rational integer a* (mod $\mathfrak{p}$), (4.13) *and* (4.14) *hold; otherwise we have*

(4.19) $$\phi_m(\alpha,\ \zeta)\equiv 1\qquad(\text{mod } \mathfrak{p}^e).$$

In particular if $N\mathfrak{p}=p$, (4.13) *and* (4.14) *apply.*

REFERENCES

[1] G. S. Ely, Some notes on the numbers of Bernoulli and Euler, American Journal of Mathematics, Vol. 5 (1880), pp. 337-341.

[2] G. Frobenius, Über die Bernoulli'schen Zahlen und die Euler'schen Polynome, Sitzungsberichte der Preussischen Akademie der Wissenschaften (1910), pp. 809-847.

[3] W. L. G. Glaisher, On the residues of the sums of the inverse powers of numbers in arithmetical progression, Quarterly Journal of Mathematics, Vol. 32 (1901), pp. 271-305.

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

[5] N. E. Nörlund, Vorlesungen über Differenzenrechnung, Berlin, 1924.

Duke University

https://doi.org/10.1017/S0027763000018043 Published online by Cambridge University Press