A SPECIAL DETERMINANT

L. CARLITZ

Let p be a prime and let $R(r)$ denote the least non-negative residue of r (mod p). The properties of Maillet's determinant (for references see [2]) $D_p = |R(rs')|$ $(r, s = 1, \cdots, (p-1)/2)$ where $ss' \equiv 1$ (mod p), suggest that it may be of interest to discuss the determinant

$$(1) \qquad \Delta_k = |R((r-s)^k)| \qquad (r, s = 0, \cdots, p-1; 1 \leqq k \leqq p-1).$$

Clearly Δ_k is a circulant. Consequently

$$(2) \qquad \Delta_k = \sum_{r=1}^{p-1} R(r^k) \cdot \prod_{s=1}^{p-1} \sum_{r=1}^{p-1} R(r^k) \epsilon^{rs}, \qquad \text{where } \epsilon = e^{2\pi i/p}.$$

Now by the binomial theorem

$$(3) \qquad (1 - \epsilon)^{p-1-k} \equiv \sum_{r=0}^{p-1-k} \frac{(k+1)\cdots(k+r)}{r!} \epsilon^r$$

$$\equiv \sum_{r=0}^{p-1-k} \frac{(r+1)\cdots(r+k)}{k!} \epsilon^r \qquad (\text{mod } p).$$

Next recall that (see for example [3, p. 207])

$$(4) \qquad x^k = \sum_{s=1}^{k} a_{ks} \binom{x+s-1}{k} \qquad (a_{ks} = a_{k,k-s+1}, \ k \geqq 1),$$

where the a_{ks} (Eulerian coefficients) are positive integers; clearly (4) implies

$$(5) \qquad \sum_{s=1}^{k} a_{ks} = k!.$$

Then using (3) and (4) we get

$$(6) \qquad (1 - \epsilon)^{p-1-k} \sum_{s=1}^{k} a_{ks} \epsilon^{s-1} \equiv \sum_{r,s} \binom{r+k}{k} a_{ks} \epsilon^{r+s-1}$$

$$= \sum_{t=1}^{p-1} \epsilon^{t-1} \sum_{s=1}^{k} a_{ks} \binom{t-s+k}{k}$$

$$\equiv \sum_{t=1}^{p-1} t^k \epsilon^{t-1} \qquad (\text{mod } p).$$

Also it is clear from (5) that

(7)
$$\sum_{s=1}^{k} a_{ks}\epsilon^{s-1} \equiv \sum_{s=1}^{k} a_{ks} \equiv k! \qquad (\mathrm{mod}\ 1 - \epsilon).$$

Thus it follows from (6) and (7) that the number

$$\alpha = \sum_{t=1}^{p-1} t^k \epsilon^{t-1}$$

is divisible by $(1-\epsilon)^{p-1-k}$ and not by $(1-\epsilon)^{p-k}$. We recall that in the cyclotomic field generated by ϵ we have the prime ideal factorization

$$(p) = (1 - \epsilon)^{p-1}.$$

Now in the double product in the right member of (2), the sum

$$\sum_{r=1}^{p-1} R(r^k)\epsilon^{rs} \equiv \epsilon^s \sum_{r=1}^{p-1} r^k \epsilon^{s(r-1)} \qquad (\mathrm{mod}\ p)$$

and is therefore divisible by exactly $(1-\epsilon)^{p-1-k}$. More precisely by (7)

$$\sum_{r=1}^{p-1} R(r^k)\epsilon^{rs} \equiv \epsilon^s k!\ (1 - \epsilon)^{p-1-k} \qquad (\mathrm{mod}\ (1 - \epsilon)^{p-k})$$

and therefore

$$(1 - \epsilon)^{-p+1+k} \sum_{r=1}^{p-1} R(r^k)\epsilon^{rs} \equiv \epsilon^s k! \qquad (\mathrm{mod}\ 1 - \epsilon).$$

Multiplying together these congruences we get

(8)
$$p^{-p+1+k} \prod_{s=1}^{p-1} \sum_{r=1}^{p-1} R(r^k)\epsilon^{rs} \equiv (k!)^{p-1} \equiv 1 \qquad (\mathrm{mod}\ 1 - \epsilon).$$

Since the left number is a rational integer, (8) holds (mod p). Thus substituting in (2) it is clear that for $k < p-1$

(9)
$$\Delta_k \equiv p^{p-1-k} \sum_{r=1}^{p-1} R(r^k) \qquad (\mathrm{mod}\ p^{p-k+1}).$$

Put

$$S_k = \sum_{r=1}^{p-1} R(r^k);$$

since $p\,|\,S_k$, $p^2\nmid S_k$ for $1 \leq k < p-1$, it follows from (9) that

(10)
$$p^{p-k}\,|\,\Delta_k,\quad p^{p-k+1}\nmid \Delta_k \qquad (1 \leq k < p - 1).$$

To get a more precise result, note first that if $a = (k, p-1)$, then $S_k = S_a$. Put $p - 1 = ab$; then in the first place

$$(11) \qquad\qquad S_a = p(p-1)/2 \qquad\qquad (b \text{ even}).$$

For b odd, on the other hand, we may prove by the method used in [1] that

$$(12) \qquad\qquad S_a \equiv -\frac{p}{2} + p\sum_u \frac{B_{bu+1}}{bu+1} \qquad\qquad (\text{mod } p^2),$$

where B_m denotes a Bernoulli number in the even suffix notation, and the summation is over $u = 1, 3, \cdots, a-1$.

We remark that for $k = p - 1$ we have the easily verified formula

$$\Delta_{p-1} = |1 - \delta_{rs}| = p - 1,$$

where δ_{rs} is the Kronecker delta. Also for $k = 1$ we have the exact result

$$\Delta_1 = (p-1)p^{p-1}/2.$$

It follows from (2) and (8) that Δ_k never vanishes.

REFERENCES

1. L. Carlitz, *The first factor of the class number of a cyclic field*, Canadian Journal of Mathematics vol. 6 (1954) pp. 23–26.

2. L. Carlitz and F. R. Olson, *Maillet's determinant*, Proc. Amer. Math. Soc. vol. 6 (1955) pp. 265–269.

3. J. Worpitzky, *Studien über die Bernoullischen und Eulerschen Zahlen*, J. Reine Angew. Math. vol. 94 (1883) pp. 202–322.

DUKE UNIVERSITY