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

\[
\Delta_k = |R((r - s)^k)| \quad (r, s = 0, \cdots, p - 1; 1 \leq k \leq p - 1).
\]

Clearly \( \Delta_k \) is a circulant. Consequently

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

Now by the binomial theorem

\[
(1 - \epsilon)^{p-1-k} = \sum_{r=0}^{p-1-k} \binom{k+1}{r+1} \cdots \binom{k+r}{r+1} \epsilon^r \equiv \sum_{r=0}^{p-1-k} \binom{r+1}{k} \cdots \binom{r+k}{k} \epsilon^r \quad \text{(mod } p). \]

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

\[
x^k = \sum_{s=1}^{k} a_{ks} \binom{x + s - 1}{k} \quad (a_{ks} = a_{k,k-s+1}, \quad k \geq 1),
\]

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

\[
\sum_{i=1}^{k} a_{ks} = k!.
\]

Then using (3) and (4) we get

\[
(1 - \epsilon)^{p-1-k} \sum_{s=1}^{k} a_{ks} \epsilon^{s-1} = \sum_{r,s} \binom{r+k}{k} a_{ks} \epsilon^{r+s-1} \equiv \sum_{t=1}^{p-1} \epsilon^{t-1} \sum_{s=1}^{k} a_{ks} \binom{t-s+k}{k} \quad \text{(mod } p). \]

Received by the editors May 25, 1954.

270
Also it is clear from (5) that

\[ \sum_{i=1}^{k} a_{ik} e^{r-1} \equiv \sum_{i=1}^{k} a_{ke} \equiv k! \quad (\text{mod } 1 - e). \]

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

\[ \alpha = \sum_{i=1}^{p-1} t^i e^{r-1} \]

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

\[ (p) = (1 - e)^{p-1}. \]

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

\[ \sum_{r=1}^{p-1} R(rk)e^{r} \equiv e^{*} \sum_{r=1}^{p-1} r^k e^{(r-1)} \quad (\text{mod } p) \]

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

\[ \sum_{r=1}^{p-1} R(rk)e^{r} \equiv e^{*} k! (1 - e)^{p-1-k} \quad (\text{mod } (1 - e)^{p-k}) \]

and therefore

\[ (1 - e)^{-p+k+1} \sum_{r=1}^{p-1} R(rk)e^{r} \equiv e^{*} k! \quad (\text{mod } 1 - e). \]

Multiplying together these congruences we get

\[ p^{-p+k+1} \prod_{r=1}^{p-1} \sum_{r=1}^{p-1} R(rk)e^{r} = (k!)^{p-1} = 1 \quad (\text{mod } 1 - e). \]

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

\[ \Delta_k \equiv p^{p-k} \sum_{r=1}^{p-1} R(rk) \quad (\text{mod } p^{p-k+1}). \]

Put

\[ S_k = \sum_{r=1}^{p-1} R(rk); \]

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

\[ p^{p-k} | \Delta_k, \quad p^{p-k+1} \not| \Delta_k \quad (1 \leq k < p - 1). \]
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

\[
S_a = \frac{p(p - 1)}{2} \quad \text{ (} b \text{ even).}
\]

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

\[
S_a = -\frac{p}{2} + p \sum_u \frac{B_{bu+1}}{bu + 1} \quad \text{ (mod } p^2),
\]

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

We remark that for \( k = p - 1 \) we have the easily verified formula

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

where \( \delta_{rs} \) 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 \( \Delta_k \) never vanishes.

References


Duke University