A DETERMINANT CONNECTED WITH FERMAT'S LAST THEOREM

L. CARLITZ

1. Put

$$\Delta_n = \begin{vmatrix} 1 & C_{n,1} & C_{n,2} & \cdots & C_{n,n-1} \\ C_{n,n-1} & 1 & C_{n,1} & \cdots & C_{n,n-2} \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ C_{n,1} & C_{n,2} & C_{n,3} & \cdots & 1 \end{vmatrix},$$

where the $C_{n,k}$ are binomial coefficients. Bachmann has proved that if p is an odd prime and Δ_{p-1} is not divisible by p^2, then the equation $x^p+y^p+z^p=0$ has no solutions prime to p. Lubelski has proved that for $p \geqq 7$, Δ_{p-1} is indeed divisible by p^s so that Bachmann's criterion is otiose. E. Lehmer has proved the stronger result that Δ_{p-1} is divisible by $p^{p-2}q_2$ for every prime p, where $q_2=(2^{p-1}-1)/p$. Moreover, she proved that $\Delta_n=0$ if and only if $n=6k$. For references see [2].

In view of the above it may be of interest to determine the residue of Δ_{p-1} (mod p^{p-1}). Since Δ_n is a circulant, it follows that

$$\Delta_{p-1} = \prod_{j=1}^{p-1} \left\{ (1+\epsilon^j)^{p-1} - 1 \right\}, \tag{1}$$

where ϵ is any primitive $(p-1)$st root of unity. Since

$$\prod_{j=1}^{p-1}{}'(1+\epsilon^j) = p-1,$$

where the prime denotes that $j \neq (p-1)/2$, (1) becomes

$$\Delta_{p-1} = -\frac{2^p-2}{p-1} \prod_{j=1}^{p-2}{}' \left\{ (1+\epsilon^j)^p - (1+\epsilon^j) \right\}. \tag{2}$$

Now

$$\begin{aligned} \frac{(1+\epsilon^j)^p - (1+\epsilon^j)}{p} &= \sum_{s=1}^{p-1} \binom{p-1}{s-1} \frac{\epsilon^{sj}}{s} \\ &\equiv \sum_{s=1}^{p-1} (-1)^{s-1} \frac{\epsilon^{sj}}{s} \qquad \pmod{p}. \end{aligned}$$

Let Z denote the cyclotomic field $R(\epsilon)$, where R is the rational field.

Received by the editors September 29, 1958.

It is known that in Z the prime p is a product of $\phi(p-1)$ distinct prime ideals of the first degree. If $\mathfrak{p}$ denotes one of the prime ideals dividing p, then we have

$$\mathfrak{p} = (p, \epsilon - r),$$

where r is a primitive root (mod p). Then

$$\epsilon \equiv r \qquad (\mathfrak{p}), \tag{3}$$

so that

$$\frac{(1+\epsilon^j)^p - (1+\epsilon^j)}{p} \equiv \sum_{s=1}^{p-1} (-1)^{s-1} \frac{r^{sj}}{s} \qquad (\mathfrak{p}).$$

Substituting in (2) we get

$$\Delta_{p-1} \equiv (2^p - 2)p^{p-3} \prod_{j=1}^{p-2}{}' \sum_{s=1}^{p-1} (-1)^{s-1} \frac{r^{sj}}{s} \qquad (p^{p-2}\,\mathfrak{p}).$$

Since both members are rational numbers that are integral (mod p) this implies

$$\Delta_{p-1} \equiv (2^p - 2)p^{p-3} \prod_{a=2}^{p-2} \sum_{s=1}^{p-1} (-1)^{s-1} \frac{a^s}{s} \qquad (\text{mod } p^{p-1}). \tag{4}$$

If we put

$$q(a) = \frac{a^{p-1} - 1}{p} \qquad (p \nmid a),$$

then

$$(1+a)q(1+a) - aq(a) \equiv \sum_{s=1}^{p-1} (-1)^{s-1} \frac{a^s}{s} \qquad (\text{mod } p),$$

so that (4) becomes

$$\Delta_{p-1} \equiv (2^p - 2)p^{p-3} \prod_{a=2}^{p-2} \{(1+a)q(1+a) - aq(a)\} \qquad (\text{mod } p^{p-1}) \tag{5}$$

or if we prefer

$$\Delta_{p-1} \equiv p^{p-2} \prod_{a=1}^{p-2} \{(1+a)q(1+a) - aq(a)\} \qquad (\text{mod } p^{p-1}). \tag{6}$$

It follows from (6) that $\Delta_{p-1} \equiv 0$ (mod p^{p-1}) if and only if for some a, $1 \leqq a \leqq p-2$,

$$(1+a)q(1+a) \equiv aq(a) \qquad (\text{mod } p) \tag{7}$$

or equivalently

$$\sum_{s=1}^{p-1}(-1)^{s-1}\frac{a^s}{s}\equiv 0 \qquad (\text{mod } p). \tag{8}$$

For $p\equiv 1$ (mod 6), the condition (7) is satisfied by picking a such that $a^2+a+1\equiv 0$ (mod p), as is easily verified. This is in agreement with Mrs. Lehmer's second result.

2. Another expression for the residue of Δ_{p-1} (mod p^{p-1}) can be obtained by slightly modifying Mrs. Lehmer's second method. Namely to each element of the kth column of Δ_{p-1} we add the corresponding element of the $(k+1)$st column for $k=1, 2, \cdots, p-2$. Then each element of the first $p-2$ columns contains the factor p. After a little manipulation we find that

$$p^{-(p-2)}\Delta_{p-1}\equiv |A_{r,s}| \qquad (\text{mod } p), \tag{9}$$

where

$$A_{r,s}=\begin{cases}\dfrac{(-1)^{r-s}}{s-r+1} & (s\geqq r),\\[2ex] \dfrac{(-1)^{r-s}}{p+s-r} & (s<r)\end{cases}$$

when $s\leqq p-2$, while for $s=p-1$

$$A_{r,p-1}=(-1)^r.$$

Removing the negative signs and adding the first $p-2$ rows to the last row, (9) reduces to

$$\Delta_{p-1}\equiv -p^{p-2}D \qquad (\text{mod } p^{p-1}), \tag{10}$$

where

$$D=\begin{vmatrix} 1 & \dfrac{1}{2} & \dfrac{1}{3} & \cdots & \dfrac{1}{p-2}\\[2ex] \dfrac{1}{p-1} & 1 & \dfrac{1}{2} & \cdots & \dfrac{1}{p-3}\\[2ex] \dfrac{1}{p-2} & \dfrac{1}{p-1} & 1 & \cdots & \dfrac{1}{p-4}\\ \cdot & \cdot & \cdot & \cdots & \cdot\\ \dfrac{1}{3} & \dfrac{1}{4} & \dfrac{1}{5} & \cdots & 1\end{vmatrix}. \tag{11}$$

Note that D is not quite a circulant.

Now consider the circulant of order $p-1$

$$C(x_0, x_1, \cdots, x_{p-2}) = \left| x_{k-j} \right| \qquad (j, k = 0, 1, \cdots, p-2),$$

where $x_j = x_{j-p+1}$. Analogous to the factorization of a circulant we have

$$C(x_0, x_1, \cdots, x_{p-2}) \equiv \prod_{j=0}^{p-2} \sum_{k=0}^{p-2} r^{jk} x_k \qquad (\mathrm{mod}\ p), \tag{12}$$

where r is a fixed primitive root (mod p). Suppose that

$$x_0 + x_1 + \cdots + x_{p-2} \equiv 0 \qquad (\mathrm{mod}\ p) \tag{13}$$

and define

$$C'(x_0, x_1, \cdots, x_{p-2}) = \left| x_{k-j} \right| \qquad (j, k = 0, 1, \cdots, p-3).$$

Then (12) implies

$$C'(x_0, x_1, \cdots, x_{p-2}) \equiv - \prod_{j=1}^{p-2} \sum_{k=0}^{p-2} r^{jk} x_k \qquad (\mathrm{mod}\ p). \tag{14}$$

For an analogous result compare [1].

If we take

$$x_j = \frac{1}{j+1} \qquad (j = 0, 1, \cdots, p-2),$$

(13) is satisfied, $C'(x_0, x_1, \cdots, x_{p-2})$ reduces to the determinant D defined by (11), and (14) becomes

$$D \equiv - \prod_{a=2}^{p-1} \sum_{k=0}^{p-2} \frac{a^k}{k+1} \qquad (\mathrm{mod}\ p). \tag{15}$$

This can be transformed into

$$\begin{aligned} D &\equiv \prod_{a=2}^{p-1} \sum_{k=1}^{p-1} \frac{a^k}{k} \\ &\equiv - \prod_{a=1}^{p-2} \sum_{k=1}^{p-1} (-1)^{k-1} \frac{a^k}{k} \\ &\equiv - \prod_{a=1}^{p-2} \left\{ (1+a)q(1+a) - aq(a) \right\} \qquad (\mathrm{mod}\ p). \end{aligned}$$

Thus (10) and (15) are in agreement with (6). We have therefore an alternative proof of (6).

REFERENCES

1. L. Carlitz, *Some cyclotomic determinants*, Bull. Calcutta Math. Soc. vol. 49 (1957) pp. 49–51.

2. Emma Lehmer, *On a resultant connected with Fermat's last theorem*, Bull. Amer. Math. Soc. vol. 41 (1935) pp. 864–867.

DUKE UNIVERSITY

ON THE MEASURE OF HILBERT NEIGHBORHOODS FOR PROCESSES WITH STATIONARY, INDEPENDENT INCREMENTS

GLEN BAXTER[1]

1. **Introduction.** Let $\{x(t),\ 0 \leqq t < \infty\}$ denote a stochastic process with stationary, independent increments for which $x(0)=0$. According to the Lévy-Khitchine representation, the characteristic function of $x(t)$ has the form

$$E\{e^{i\xi x(t)}\} = e^{-t\psi(\xi)}. \tag{1}$$

Moreover,

$$\psi(\xi) = -i\gamma\xi - \int_{-\infty}^{\infty}\left(e^{i\xi u} - 1 - \frac{i\xi u}{1+u^2}\right)\frac{1+u^2}{u^2}\,dG(u), \tag{2}$$

where $G(u)$ is a bounded, nondecreasing function with $G(-\infty)=0$ and where γ is a real-valued constant. Below it is shown that for certain processes of this type the measure of the Hilbert neighborhood of the origin is related to the solution of a certain differential system. In fact, (A) *if* $\{x(t),\ 0 \leqq t < \infty\}$ *is a separable stochastic process with symmetric, stationary, and independent increments for which* $x(0)=0$, *and if*

Received by the editors February 24, 1958 and, in revised form, December 8, 1958.

[1] This research was supported by the United States Air Force, through the office of Scientific Research of the Air Research and Development Command, under contract No. AF 18 (603)-30. Reproduction in whole or in part is permitted for any purpose of the United States Government.