A DETERMINANT CONNECTED WITH FERMAT'S LAST THEOREM

L. CARLITZ

1. Put

\[
\Delta_n = \begin{vmatrix}
1 & C_{n,1} & C_{n,2} & \cdots & C_{n,n-1} \\
C_{n,n-1} & 1 & C_{n,1} & \cdots & C_{n,n-2} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
C_{n,1} & C_{n,2} & C_{n,3} & \cdots & 1
\end{vmatrix},
\]

where the \( C_{n,k} \) are binomial coefficients. Bachmann has proved that if \( p \) is an odd prime and \( \Delta_{p-1} \) 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 \( p \geq 7 \), \( \Delta_{p-1} \) is indeed divisible by \( p^3 \) so that Bachmann's criterion is otiose. E. Lehmer has proved the stronger result that \( \Delta_{p-1} \) 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 \( \Delta_{p-1} \pmod{p^{p-1}} \). Since \( \Delta_n \) is a circulant, it follows that

\[
\Delta_{p-1} = \prod_{j=1}^{p-1} \left\{ (1 + e^j)^{p-1} - 1 \right\},
\]

where \( e \) is any primitive \((p-1)\)st root of unity. Since

\[
\prod_{j=1}^{p-1}' (1 + e^j) = p - 1,
\]

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

\[
\Delta_{p-1} = -\frac{2^p - 2}{p - 1} \prod_{j=1}^{p-2}' \left\{ (1 + e^j)^p - (1 + e^j) \right\}.
\]

Now

\[
\frac{(1 + e^j)^p - (1 + e^j)}{p} = \sum_{s=1}^{p-1} \frac{(p - 1) \epsilon^{sj}}{s} = \sum_{s=1}^{p-1} (-1)^{s-1} \frac{\epsilon^{sj}}{s} \pmod{p}.
\]

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

Received by the editors September 29, 1958.

686
It is known that in \( \mathbb{Z} \) the prime \( \mathfrak{p} \) is a product of \( \phi(p-1) \) distinct prime ideals of the first degree. If \( \mathfrak{p} \) denotes one of the prime ideals dividing \( \mathfrak{p} \), then we have
\[
\mathfrak{p} = (\mathfrak{p}, e - r),
\]
where \( r \) is a primitive root \((\text{mod } \mathfrak{p})\). Then
\[
\epsilon \equiv r \pmod{\mathfrak{p}},
\]
so that
\[
\frac{(1 + e^r)^p - (1 + e^r)}{\mathfrak{p}} = \sum_{s=1}^{p-1} (-1)^{s-1} \frac{r^{si}}{s} \pmod{\mathfrak{p}}.
\]
Substituting in (2) we get
\[
\Delta_{p-1} \equiv (2^p - 2) p^{p-3} \prod_{j=1}^{p-2} \sum_{s=1}^{p-1} (-1)^{s-1} \frac{r^{si}}{s} \pmod{\mathfrak{p}^{p-2}}.
\]
Since both members are rational numbers that are integral \((\text{mod } \mathfrak{p})\) this implies
\[
\Delta_{p-1} \equiv (2^p - 2) p^{p-3} \prod_{a=2}^{p-2} \sum_{s=1}^{p-1} (-1)^{s-1} \frac{a^s}{s} \pmod{\mathfrak{p}^{p-1}}.
\]
If we put
\[
q(a) = \frac{a^{p-1} - 1}{\mathfrak{p}} \quad (\mathfrak{p} \nmid a),
\]
then
\[
(1 + a)q(1 + a) - aq(a) \equiv \sum_{s=1}^{p-1} (-1)^{s-1} \frac{a^s}{s} \pmod{\mathfrak{p}},
\]
so that (4) becomes
\[
\Delta_{p-1} \equiv (2^p - 2) p^{p-3} \prod_{a=2}^{p-2} \{(1 + a)q(1 + a) - aq(a)\} \pmod{\mathfrak{p}^{p-1}}.
\]
or if we prefer
\[
\Delta_{p-1} \equiv p^{p-2} \prod_{a=1}^{p-2} \{(1 + a)q(1 + a) - aq(a)\} \pmod{\mathfrak{p}^{p-1}}.
\]
It follows from (6) that \( \Delta_{p-1} \equiv 0 \pmod{\mathfrak{p}^{p-1}} \) if and only if for some \( a, 1 \leq a \leq p - 2 \),
\[
(1 + a)q(1 + a) \equiv aq(a) \pmod{\mathfrak{p}}.
\]
or equivalently

\[(8) \sum_{s=1}^{p-1} (-1)^{s-1} \frac{a^s}{s} \equiv 0 \pmod{p}.\]

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

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

\[(9) p^{-(p-2)}\Delta_{p-1} \equiv \left| A_{r,s} \right| \pmod{p},\]

where

\[
A_{r,s} = \begin{cases} 
\frac{(-1)^{r-s}}{s-r+1} & (s \geq r), \\
\frac{(-1)^{r-s}}{p+s-r} & (s < r)
\end{cases}
\]

when \(s \leq p-2\), 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

\[(10) \Delta_{p-1} \equiv -p^{p-2}D \pmod{p^{p-1}},\]

where

\[
D = \begin{vmatrix}
1 & 1 & 1 & \cdots & 1 \\
\frac{1}{2} & \frac{1}{3} & \frac{1}{p-2} \\
\frac{1}{p-1} & 1 & \frac{1}{2} & \frac{1}{p-3} \\
\frac{1}{p-2} & \frac{1}{p-1} & 1 & \cdots & 1 \\
\frac{1}{3} & \frac{1}{4} & \frac{1}{5} & \cdots & 1
\end{vmatrix}
\]
Note that $D$ is not quite a circulant.

Now consider the circulant of order $p - 1$

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

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

$$C(x_0, x_1, \cdots, x_{p-2}) = \prod_{j=0}^{p-2} \sum_{k=0}^{p-2} r^{jk} x_k \quad (\text{mod } p),$$

where $r$ is a fixed primitive root $(\text{mod } p)$. Suppose that

$$x_0 + x_1 + \cdots + x_{p-2} \equiv 0 \quad (\text{mod } p)$$

and define

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

Then (12) implies

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

For an analogous result compare [1].

If we take

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

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

$$D \equiv - \prod_{a=2}^{p-1} \sum_{k=0}^{p-2} \frac{a^k}{k + 1} \quad (\text{mod } p).$$

This can be transformed into

$$D \equiv \prod_{a=2}^{p-1} \sum_{k=1}^{p-1} \frac{a^k}{k}$$

$$\equiv - \prod_{a=1}^{p-2} \sum_{k=1}^{p-1} (-1)^{k-1} \frac{a^k}{k}$$

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

Thus (10) and (15) are in agreement with (6). We have therefore an alternative proof of (6).
ON THE MEASURE OF HILBERT NEIGHBORHOODS FOR PROCESSES WITH STATIONARY, INDEPENDENT INCREMENTS

GLEN BAXTER

1. Introduction. Let \( \{x(t), 0 \leq t < \infty\} \) 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

\[
E\{e^{i\xi \varepsilon(t)}\} = e^{-t\psi(\xi)}.
\]

Moreover,

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

where \( G(u) \) is a bounded, nondecreasing function with \( G(-\infty) = 0 \) and where \( \gamma \) 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 \( \{x(t), 0 \leq t < \infty\} \) 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.