tinct classes. According to our bound there are at least two more such splittings obtainable in this way.

REFERENCES


REED COLLEGE

A DETERMINANT CONNECTED WITH FERMAT'S LAST THEOREM

L. CARLITZ

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 \( C_{n,r} \) are binomial coefficients. Bachmann showed that if

\[ x^p + y^p + z^p = 0 \quad (p \nmid xyz) \]

is solvable then \( \Delta_{p-1} \equiv 0 \pmod{p^3} \). However Lubelski showed that for \( p \geq 7 \), \( \Delta_{p-1} \) is divisible by \( p^8 \), while E. Lehmer proved that \( \Delta_{p-1} \) is divisible by \( p^{p-2}q_2 \), where \( q_2 = (2^{p-1} - 1)/p \); also \( \Delta_n = 0 \) if and only if \( n = 6k \). For references see [2].

The writer [1] has determined the residue of \( \Delta_{p-1} \pmod{p^{p-1}} \). The result is that

Received by the editors December 1, 1959.
1 Research supported by National Science Foundation, Grant G-9425.
\[
\Delta_{p-1} \equiv p^{p-2} \prod_{a=1}^{p-2} \{(1 + a)q(1 + a) - aq(a)\} \pmod{p^{p-1}},
\]
where
\[
q(a) = \frac{a^{p-1} - 1}{p},
\]
or if we prefer,
\[
(2) \quad \Delta_{p-1} \equiv \prod_{a=1}^{p-2} ((a + 1)^p - a^p - 1) \pmod{p^{p-1}}.
\]

Now it is known (see [3, p. 564] for references) that when (1) is solvable
\[
q(r) \equiv 0 \pmod{p}
\]
for all primes \( r \leq 43 \) and therefore for all integral \( r \leq 46 \). Mrs. Lehmer noted that it follows from
\[
q(2) \equiv 0 \pmod{p}
\]
that if (1) is solvable then \( \Delta_{p-1} \) is divisible by \( p^{p-1} \). In view of (2) it seems plausible that when (1) is solvable \( \Delta_{p-1} \) is divisible by a considerably higher power of \( p \); however since the modulus in (2) is only \( p^{p-1} \) such a result cannot be inferred without further proof.

Put \( C_r = C_{p-1,r} \) for \( 0 \leq r \leq p - 1 \) and \( C_r = C_s \) for \( r \equiv s \pmod{p - 1} \). Then
\[
\Delta_{p-1} = \left| C_{s-r} \right| \quad (r, s = 1, \ldots, p - 1).
\]
Let \( e \) be an arbitrary non-negative integer and consider the determinant
\[
D_e = \left| s^{pe} \right| \quad (r, s = 1, \ldots, p - 1).
\]
Then
\[
D_e \equiv D_0 \pmod{p};
\]
since
\[
D_0 = (p - 1)! \prod_{1 \leq r < s \leq p - 1} (r - s),
\]
it follows that
\[
D_e \not\equiv 0 \pmod{p}.
\]

Similarly the determinant
\[ D'_s = |r^{-ps}| \quad (r, s = 1, \cdots, p - 1) \]
is a rational number with both numerator and denominator prime to \( p \). Consequently
\[ (3) \quad \Delta'_{p-1} = D'_s \Delta_{p-1} D_s \]
and \( \Delta_{p-1} \) are divisible by the same power of \( p \).

We have
\[ (4) \quad D'_s \Delta_{p-1} D_s = |A_{rs}| \quad (r, s = 1, \cdots, p - 1) \]
where
\[
A_{rs} = \sum_{j,k=1}^{p-1} r^{-ps} j \sum_{k,j=1}^{p-1} \chi_{j, j} \equiv \sum_{i=1}^{p-1} C_i \sum_{k,j=1}^{p-1} r^{-ps} j \sum_{k,j=1}^{p-1} \chi_{j, j} (\text{mod } p+1). \]
Since
\[
\sum_{j=1}^{p-1} (r^{-ps} j) \chi_{j, j} \equiv (p - 1) \delta_{rs} \quad (\text{mod } p+1), \]
where \( \delta_{rs} \) is the Kronecker delta, we get
\[
A_{rs} \equiv (p - 1) \delta_{rs} \sum_{i=1}^{p-1} C_{p-1,i} \chi_{i, i} \equiv (p - 1) \delta_{rs} \{(1 + s^p)^{p-1} - 1\} \quad (\text{mod } p+1). \]
Therefore (3) and (4) imply
\[ (5) \quad \Delta'_{p-1} \equiv -(p - 1)^{p-1} \prod_{r=1}^{p-2} \{1 + r^p\}^{p-1} - 1 \quad (\text{mod } p+1). \]
Incidentally it is easily verified that
\[ D'_s D_s \equiv (p - 1)^{p-1} \quad (\text{mod } p+1), \]
so that
\[ (6) \quad \Delta'_{p-1} \equiv (p - 1)^{p-1} \Delta_{p-1} \quad (\text{mod } p+1). \]
From (5) and (6) we get
\[ (7) \quad \Delta_{p-1} = - p^{p-2} \prod_{r=1}^{p-2} q(1 + r^p) \pmod{p^{p+1}}. \]

Now if (1) is solvable we have

\[ q(a) \equiv 0 \pmod{p} \quad (2 \leq a \leq 46). \]

Also if

\[ a^p \equiv a \pmod{p^2} \]

it follows at once that

\[ (1 + a^p)^{p-1} \equiv a^{p-1} \equiv 1 \pmod{p^2} \quad (a < 46), \]

so that

\[ q(1 + a^p) \equiv 0 \pmod{p} \quad (a < 46), \]

for all \( e \geq 0 \). Hence (since \( p > 50 \)) (7) yields

\[ \Delta_{p-1} \equiv c p^{p+43} \pmod{p^{p+1}}, \]

where \( c \) is some integer. If we take

\[ e = p + 42 \]

we obtain the following

**Theorem.** If the equation

\[ x^p + y^p + z^p = 0 \]

is solvable in rational integer \( x, y, z \) each prime to \( p \) then

\[ \Delta_{p-1} \equiv 0 \pmod{p^{p+43}}. \]

We remark that the theorem is meaningful only for \( p \equiv -1 \pmod{6} \) since the determinant \( \Delta_{p-1} \) is zero when \( p \equiv 1 \pmod{6} \).

**References**


**Duke University**