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

REFERENCES

1. D. H. Lehmer, *The Tarry-Escott problem*, Scripta Math. vol. 13 (1947) pp. 37–41.

2. J. B. Roberts, *A curious sequence of signs*, Amer. Math. Monthly vol. 64 (1957) pp. 317–322.

3. ———, *A new proof of a theorem of Lehmer*, Canad. J. Math. vol. 10 (1958) pp. 191–194.

4. E. M. Wright, *Equal sums of like powers*, Edinburgh Math. Proc. vol. 8 (1949) pp. 138–142.

5. ———, *Equal sums of like powers*, Bull. Amer. Math. Soc. vol. 54 (1948) pp. 755–757.

6. ———, *Prouhet's* 1851 *solution of the Tarry-Escott problem of* 1910, Amer. Math. Monthly vol. 66 (1959) pp. 199–201.

REED COLLEGE

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 $C_{n,r}$ are binomial coefficients. Bachmann showed that if

$$x^p + y^p + z^p = 0 \qquad (p \nmid xyz) \tag{1}$$

is solvable then $\Delta_{p-1} \equiv 0 \pmod{p^3}$. However Lubelski showed that for $p \geqq 7$, Δ_{p-1} is divisible by p^8, while E. Lehmer proved that Δ_{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,

$$\Delta_{p-1} \equiv \prod_{a=1}^{p-2} ((a+1)^p - a^p - 1) \pmod{p^{p-1}}. \tag{2}$$

Now it is known (see [3, p. 564] for references) that when (1) is solvable

$$q(r) \equiv 0 \pmod{p}$$

for all primes $r \leqq 43$ and therefore for all integral $r \leqq 46$. Mrs. Lehmer noted that it follows from

$$q(2) \equiv 0 \pmod{p}$$

that if (1) is solvable then Δ_{p-1} is divisible by p^{p-1}. In view of (2) it seems plausible that when (1) is solvable Δ_{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 $0 \leqq r \leqq p-1$ and $C_r = C_s$ for $r \equiv s \pmod{p-1}$. Then

$$\Delta_{p-1} = |C_{s-r}| \qquad (r, s = 1, \cdots, p-1).$$

Let e be an arbitrary non-negative integer and consider the determinant

$$D_e = |s^{p^e r}| \qquad (r, s = 1, \cdots, p-1).$$

Then

$$D_e \equiv D_0 \pmod{p};$$

since

$$D_0 = (p-1)! \prod_{1 \leqq r < s \leqq p-1} (r - s),$$

it follows that

$$D_e \not\equiv 0 \pmod{p}.$$

Similarly the determinant

$$D_e' = |r^{-p^e s}| \qquad (r, s = 1, \cdots, p-1)$$

is a rational number with both numerator and denominator prime to p. Consequently

$$\Delta_{p-1}' = D_e' \Delta_{p-1} D_e \tag{3}$$

and Δ_{p-1} are divisible by the same power of p.

We have

$$D_e' \Delta_{p-1} D_e = |A_{rs}| \qquad (r, s = 1, \cdots, p-1). \tag{4}$$

where

$$\begin{aligned} A_{rs} &= \sum_{j,k=1}^{p-1} r^{-p^e j} C_{k-j} s^{p^e k} \\ &= \sum_{t=1}^{p-1} C_t \sum_{k-j=t} r^{-p^e j} s^{p^e k} \\ &\equiv \sum_{t=1}^{p-1} C_t \sum_{j=1}^{p-1} (r^{-p^e} s^{p^e})^j s^{p^e t} \pmod{p^{e+1}}. \end{aligned}$$

Since

$$\sum_{j=1}^{p-1} (r^{-p^e} s^{p^e})^j \equiv (p-1)\delta_{rs} \pmod{p^{e+1}},$$

where δ_{rs} is the Kronecker delta, we get

$$\begin{aligned} A_{rs} &\equiv (p-1)\delta_{rs} \sum_{t=1}^{p-1} C_{p-1,t} s^{p^e t} \\ &\equiv (p-1)\delta_{rs}\{(1 + s^{p^e})^{p-1} - 1\} \pmod{p^{e+1}}. \end{aligned}$$

Therefore (3) and (4) imply

$$\Delta_{p-1}' \equiv -(p-1)^{p-1} \prod_{r=1}^{p-2} \{(1 + r^{p^e})^{p-1} - 1\} \pmod{p^{e+1}}. \tag{5}$$

Incidentally it is easily verified that

$$D_e' D_e \equiv (p-1)^{p-1} \pmod{p^{e+1}},$$

so that

$$\Delta_{p-1}' \equiv (p-1)^{p-1} \Delta_{p-1} \pmod{p^{e+1}}. \tag{6}$$

From (5) and (6) we get

$$\Delta_{p-1} \equiv - p^{p-2} \prod_{r=1}^{p-2} q(1 + r^{p^e}) \pmod{p^{e+1}}. \tag{7}$$

Now if (1) is solvable we have

$$q(a) \equiv 0 \pmod{p} \qquad (2 \leqq a \leqq 46).$$

Also if

$$a^p \equiv a \pmod{p^2}$$

it follows at once that

$$(1 + a^{p^e})^{p-1} \equiv a^{p-1} \equiv 1 \pmod{p^2} \qquad (a < 46),$$

so that

$$q(1 + a^{p^e}) \equiv 0 \pmod{p} \qquad (a < 46),$$

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

$$\Delta_{p-1} \equiv c p^{p+43} \pmod{p^{e+1}},$$

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 Δ_{p-1} is zero when $p \equiv 1 \pmod{6}$.

REFERENCES

1. L. Carlitz, *A determinant connected with Fermat's last theorem*, Proc. Amer. Math. Soc. vol. 10 (1959) pp. 686–690.

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

3. H. S. Vandiver, *Fermat's last theorem. Its history and the nature of the known results concerning it*, Amer. Math. Monthly vol. 43 (1946) pp. 555–578.

DUKE UNIVERSITY