AN EXTENSION OF FERMAT'S THEOREM

Chinthayamma and J. M. Gandhi

(received December 12, 1966)

In [1] Trypanis has proved the following extension of Fermat's theorem: If a is any integer, p a prime, $p \nmid a$, then

$$a^{(p-1)/p^n} \equiv 1 \pmod{p^{1/p^n}} . \tag{1}$$

This result is to be understood in the sense that $a^{(p-1)/p^n} - 1 = p^{1/p^n}\alpha$ where α is an algebraic integer. In [2] L. Carlitz has proved the following: Let $\phi(p^e) | w$ where p is a prime and $\lambda \geq e$ be the greatest integer such that $a^w \equiv 1 \pmod{p^\lambda}$. Then

$$\Delta^r a^{n^k} = \sum_{s=0}^{r} (-1)^{r-s} \binom{r}{s} a^{(n+sw)^k} \equiv 0 \pmod{p^{\lambda r_k}} , \tag{2}$$

where $r_k = [\frac{r+k-1}{k}]$. Combining (1) and (2) we prove the following extension of Fermat's theorem.

THEOREM. Let λ be the greatest integer, greater than or equal to 1 such that $a^{(p-1)/p^n} \equiv 1 \pmod{p^{\lambda/p^n}}$ where a is an integer, p a prime and $p \nmid a$. Then

$$\Delta^r a^{t^k} = \sum_{s=0}^{r} (-1)^{r-s} \binom{r}{s} a^{(t+(p-1)s/p^n)^k} \equiv 0 \pmod{p^{\lambda/p^n r_k}} , \tag{3}$$

where $r_k = [\frac{r+k-1}{k}]$ and t is an integer.

https://doi.org/10.4153/CMB-1967-036-8 Published online by Cambridge University Press

At the end of the paper we have given some more generalizations of the present theorem.

First we prove a lemma from which the theorem can be easily proved.

LEMMA. Let

$$f(x) = \sum_{s=0}^{r} (-1)^{r-s} \binom{r}{s} x^{a_1 s + a_2 s^2 + \ldots + a_k s^k} \tag{4}$$

where the a_J are arbitrary non-negative algebraic integers and $k \geq 1$. Then

$$f(x) = (x-1)^{r_k} g(x), \tag{5}$$

where $g(x)$ is a polynomial with algebraic integer co-efficients. Moreover, if $r = km$ then

$$g(1) = \frac{r!}{m!} a_k^m . \tag{6}$$

<u>Proof.</u> For $r \geq 1$, $f(1) = \sum_{s=0}^{r} (-1)^{r-s} \binom{r}{s} = 0$.

Let $1 \leq J < r_k$. Then for the J^{th} derivative, we have

$$d^J f(1) = \sum_{s=0}^{r} (-1)^{r-s} \binom{r}{s} \prod_{i=0}^{J-1} (a_1 s + a_2 s^2 + \ldots + a_k s^k - i) . \tag{7}$$

Setting

$$\sum_{i=0}^{J-1} (a_1 s + a_2 s^2 + \ldots + a_k s^k - i) = A_o^{(J)} + A_1^{(J)} s + A_2^{(J)} s(s-1) + \ldots + A_\ell^{(J)} s(s-1) \ldots (s-\ell+1) , \tag{8}$$

where $\ell = JK \leq \frac{r_k - 1}{k} < r$ and the $A_i(J)$ are algebraic integers, (6) becomes

https://doi.org/10.4153/CMB-1967-036-8 Published online by Cambridge University Press

$$d^J f(1) = \sum_{s=0}^{r} (-1)^{r-s} \binom{r}{s} \sum_{i=0}^{\ell} A_i^{(J)} s(s-1) \ldots (s-i+1)$$

$$(9) \qquad = \sum_{i=0}^{\ell} A_i^{(J)} r(r-1) \ldots (r-i+1) \sum_{s=i}^{r} (-1)^{r-s} \binom{r-i}{s-i}$$

$$= 0 \quad \text{since } \ell < r \ .$$

Hence the result (5).

Next, when $r = km$, $r_k = m$, from (9).

$$d^m f(1) = \sum_{i=0}^{r} A_i^{(m)} r(r-1) \ldots (r-i+1) \sum_{s=i}^{r} (-1)^{r-s} \binom{r-i}{s-i}$$

$$(10) \qquad = r!\, A_i^{(m)} \ .$$

Since (8) is an identity in s, $A_i^{(m)} = a_k^m$ and therefore (10) becomes $d^m f(1) = r!\, a_k^m$. But by (5) $d^m f(1) = m!\, g(1)$ and therefore $g(1) = r!/m!\, a_k^m$. Now we prove the theorem.

$$\Delta^r a^{t^k} = a^{t^k} \sum_{s=0}^{r} (-1)^{r-s} \binom{r}{s} a^{[(p-1)/p^n][(s(p-1)/p^n + t)^k - t^k]/[(p-1)/p^n]}$$

$$(11) \qquad = a^{t^k} \sum_{s=0}^{r} (-1)^{r-s} \binom{r}{s} a^{[(p-1)/p^n]\, F(s)} ,$$

where $F(s) = \sum_{J=1}^{k} \binom{k}{j} t^{k-J} s^J ((p-1)/p^n)^{J-1}$.

Now applying the lemma to (11) we get

$$\Delta^r a^{t^k} = a^{t^k} (a^{(p-1)/p^n} - 1)^{r_k} g(a^{(p-1)/p^n}) \ .$$

By (1) $\Delta^r a^{t^k} \equiv 0 \pmod{p^{\lambda r_k/p^n}}$ whereby our theorem has been proved.

Now following the method of Carlitz [2], the following theorems can be easily proved.

THEOREM 2. If the hypotheses of theorem 1 are satisfied then $\Delta^r a^{t^k} \equiv 0 \mod p^{(\lambda/p^n)r_k} + \min(\lambda/p^n)\mu$ where μ is the highest power of p dividing $r!/t!((p-1)/p^n)^{(k-1)t}$.

It may be noted that in many cases μ may be zero.

THEOREM 3. Let $k > 1$ and $r \geq 1$. Then the congruence

$$\Delta^r a^{t^k} \equiv 0 \pmod{p^{(\lambda/p^n)r_k}}$$

is best possible if and only if $\frac{r!}{r_k} \not\equiv 0 \mod p^{1/p^n}$.

REFERENCES

1. A.A. Trypanis, An extension of Fermat's Theorem. Am. Math. Monthly, 57 (1950), 87-89.

2. L. Carlitz, An extension of the Fermat theorem. Am. Math. Monthly 70 (1963), 247-250.

3. A. Hausner, Note on "An Extension of Fermat's Theorem". Am. Math. Monthly 70 (1963), 293-294.

University of Alberta, Edmonton

https://doi.org/10.4153/CMB-1967-036-8 Published online by Cambridge University Press