SIMULTANEOUS LINEAR FACTORS OF A BINOMIAL (MOD M)

BY MARTIN R. BATES AND FRANK R. OLSON

1. Introduction. It is a well-known consequence of Fermat's Theorem [3; 63, Theorem 72] that $x^{\phi(M)} - 1 \equiv 0 \pmod{M}$ has $\phi(M)$ distinct roots corresponding to the set of numbers less than and relatively prime to M. But this does not imply that $x^{\phi(M)} - 1$ has $\phi(M)$ simultaneous linear factors (mod M) [3; 99]. In particular, if $M = 9$, it may be shown that $x^6 - 1 \equiv (x - 1)(x - 2)(x^4 + 3x^3 + 7x^2 + 6x + 4) \pmod{9}$, where the quartic expression has no linear factors (mod 9). Alternative choices of linear factors for $x^6 - 1$ give rise to similar quartic factors which have no linear factors. However, there are related cases where relatively many linear factors appear. For example, since -3 is a primitive 10-th root of unity (mod 121), $x^{10} - 1 \equiv \prod_{i=1}^{10} (x - (-3)^i)$ (mod 121). Thus $x^{10} - 1$ has a full complement of ten linear factors, (mod 121). These facts led us to examine the simultaneous linear factors of the binomial expression $x^m - 1$ (mod M). This investigation supplements some results by Bauer [1], who discussed the cases $m = \phi(n)$, $M \mid n$, such that the binomial expression has a full complement of m linear factors.

In particular, if $M = p^n$ and $m = \phi(p^r)$, (where p is an odd prime, and $0 < r \leq n$), we show that factorizations of $x^m - 1$ (mod M) exist with $p - 1$ linear factors $(x - a_k)$, $1 \leq k \leq p - 1$; where the a_k are appropriate representatives of the respective residue classes $1, 2, 3, \cdots p - 1$ (mod p). Furthermore, no factorizations exist with more than $p - 1$ linear factors in these cases.

We also show that for $M = p^n$ and $m = p^s\phi(p^n)$, $s \geq 1$, factorizations exist with p^s linear factors $(x - a_k)$ corresponding to each of the $p - 1$ residue classes $a_k \equiv k \pmod{p}$ and that no such factorizations exist with $p^s + 1$ linear factors $(x - a_k)$ belonging to a given residue class $a_k \equiv k \pmod{p}$. The corresponding results for the case $M = 2^n$ are also presented. In the course of this discussion, a generalization of Lagrange's Theorem [3; 86–87, Theorem 112] is provided as follows:

THEOREM 1. *If* $a_j \equiv j \pmod{p}$, *where* p *is prime, then*

$$x^{\phi(p^n)} - 1 \equiv \prod_{j=1}^{p-1} (x^{p^{n-1}} - a_j^{p^{n-1}}) \pmod{p^n}. \tag{1}$$

2. Residue classes involving prime power exponentiation. We shall make liberal use of the fact [3; 65, Theorem 78] that $a \equiv b \pmod{p^r}$ implies $a^{p^t} \equiv b^{p^t} \pmod{p^{r+t}}$. In fact, the slightly sharper result given in Lemma 1 will be needed.

Received May 2, 1969. Mr. Bates is a graduate student at the State University of New York at Buffalo. Professor Olson was a faculty member of that institution when this research was initiated.