Internat. J. Math. & Math. Sci.
Vol. 3 No. 2 (1980) 397-400

RESEARCH NOTES

BINOMIAL EXPANSIONS MODULO PRIME POWERS

PAUL W. HAGGARD

Department of Mathematics
East Carolina University
Greenville, North Carolina 27834
U. S. A.

JOHN O. KILTINEN

Department of Mathematics
Northern Michigan University
Marquette, Michigan 49855
U. S. A.

(Received December 3, 1979)

ABSTRACT: In this note a result is given and proved concerning binomial expansions modulo prime powers. In the proof congruence modulo prime powers is generalized to the rational numbers via valuations.

KEY WORDS AND PHRASES: *Modulo Prime Powers, p-adic valuation, and rings of characteristics* p^m.

1980 MATHEMATICS SUBJECT CLASSIFICATION CODES: 10C20.

1. INTRODUCTION.

It is well known that if R is a commutative ring of prime characteristic p, then

$$(x + y)^{p} = x^{p} + y^{p} , \tag{1.1}$$

and more generally,

$$(x + y)^{p^n} = x^{p^n} + y^{p^n} , \tag{1.2}$$

for any x and y in R. The reason that (2) holds is that

$$C(p^n,k) \equiv \begin{cases} 0 & \text{if } 1 \le k \le p^n-1 \\ 1 & \text{if } k = 0 \text{ or } p^n \end{cases} \pmod{p}., \tag{1.3}$$

and so the interior terms all vanish when one applies the usual binomial expansion formula.

One cannot expect such a simple expansion with a non-prime characteristic. However, a generalization of (1.3) leads to a recognition of the vanishing terms in the case of a ring of prime power characteristic.

To develop this result, we use the notation v_p to denote the usual p-adic valuation on the rational numbers Q: $v_p(k)$ is the highest power of p dividing an integer k and $v_p(j/k) = v_p(j) - v_p(k)$ for a rational number j/k. (Set $v_p(0) = \infty$. Recall that $v_p(x + y) \geq \min\{v_p(x),v_p(y)\}$ and $v_p(xy) = v_p(x) + v_p(y)$ for any x, y in Q.) For $x, y \in Q$ and positive integer m, define $x \equiv y \pmod{p^m}$ iff $v_p(x - y) \ge m$. One can show that this defines an equivalence relation on Q which reduces to the usual equivalence relation modulo p^m on the integers Z. We will need the following fact about this relation:

For all $x, y \in Q$ and $j, k \in Z$, if $x \equiv j \pmod{p^m}$
and $y \equiv k \pmod{p^m}$,
then $xy \equiv jk \pmod{p^m}$. (1.4)

2. MAIN RESULTS:

THEOREM: For p a prime, m and n positive integers with $n \geq m-1$, and for $0 \le k \le p^n$,

$$C(p^n,k) \equiv \begin{cases} 0 & \text{if } p^{n-m+1} \nmid k \ \ (\text{ie, } v_p(k) \le n-m) \\ C(p^{m-1},i) & \text{if } k = i\cdot p^{n-m+1} \end{cases} \pmod{p^m} \tag{2.1}$$

PROOF: Note first that

$$v_p(C(p^n,k)) = v_p(\frac{p^n}{k}) = n - v_p(k). \tag{2.2}$$

To see this, write

$$C(p^n,k) = \frac{p^n}{k}\cdot\frac{p^n-1}{1}\cdot\frac{p^n-2}{2}\cdot\cdot\cdot\frac{p^n-(k-1)}{k-1}.$$

Note that $p^j \mid i$ iff $p^j \mid (p^n-i)$ for $1 \le i \le k-1$. Thus, $v_p((p^n-i)/i) = 0$ for $1 \le i \le k-1$, and so (2.2) follows.

Now if $v_p(k) \le n-m$, then from (2.2), $v_p(C(p^n,k)) \ge n-(n-m) = m$, so $C(p^n,k) \equiv 0 \pmod{p^m}$, and this case is proven.

Now take $k = i\cdot p^{n-m+1}$. Write $C(p^n,i\cdot p^{n-m+1})$ in the following form, grouping the terms divisible by p^{n-m+1} to the front:

$$C(p^n,i\cdot p^{n-m+1}) = \frac{(p^n-(i-1)p^{n-m+1})}{p^{n-m+1}}\cdot\frac{(p^n-(i-2)p^{n-m+1})}{2\cdot p^{n-m+1}}\cdot\cdot\cdot\frac{p^n}{i\cdot p^{n-m+1}}\cdot\prod\frac{p^n-j}{j}$$

The concluding product is taken over those j less than $i\cdot p^{n-m+1}$ such that $p^{n-m+1} \nmid j$. Note that the first i terms reduce to $C(p^{m-1},i)$ when all factors of p^{n-m+1} are removed. Also, since $(p^n-j)/j + 1 = p^n/j$ and $v_p(p^n/j) = n-v_p(j) \ge n-(n-m) = m$, one has $(p^n-j)/j \equiv -1 \pmod{p^m}$ for all of the terms in the concluding product. Since there are $i\cdot p^{n-m+1} - i = i(p^{n-m+1} - 1)$ such terms in the product, by (1.4), one has

$$C(p^n,i\,p^{n-m+1}) \equiv C(p^{m-1},i)\cdot(-1)^{i(p^{n-m+1}-1)} \pmod{p^m}.$$

For p odd or i even, this gives the desired result.

The one remaining case is $p = 2$ and i odd. Now by (2.2) and since i is odd, $v_2(C(2^n,i\cdot 2^{n-m+1})) = v_2(2^n/i\cdot 2^{n-m+1}) = m-1$. Thus, $C(2^n,i\cdot 2^{n-m+1})$ is 2^{m-1} times some odd integer, say $2x+1$. Then

$$C(2^n,i\cdot 2^{n-m+1}) = 2^m x + 2^{m-1} \equiv 2^{m-1} \pmod{2^m}$$

for any $n \ge m-1$. Equating for each such n to the special case $n = m-1$, one gets $C(2^n,i\cdot 2^{n-m+1}) \equiv C(2^{m-1},i) \pmod{2^m}$, which is the desired result again.

This theorem yields the following binomial expansion in rings of characteristic p^m.

COROLLARY: If R is a commutative ring of characteristic p^m and if $n \geq m-1$, then for any x and y in R,

$$(x + y)^{p^n} = \sum_{i=0}^{p^{m-1}} C(p^{m-1},i) \cdot x^{(p^{m-1}-i)p^{n-m+1}} \cdot y^{i \cdot p^{n-m+1}} . \tag{2.3}$$

Note that the number of nonvanishing terms depends only on the characteristic p^m and not on the exponent p^n, and that for $m = 1$, (2.3) reduces to (1.2). The following reference considers some closely related questions.

REFERENCE

J. Kiltinen, Linearity of exponentiation, Math. Mag. 52 (1979), 3-9.