JOURNAL OF NUMBER THEORY 10, 263–272 (1978)

# Enumeration of Power Sums Modulo A Prime

ANDREW M. ODLYZKO

*Bell Laboratories, Murray Hill, New Jersey 07974*

AND

RICHARD P. STANLEY*

*Department of Mathematics, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139*

*Communicated by H. Zassenhaus*

Received June 14, 1977; Revised November 11, 1977

We consider, for odd primes $p$, the function $N(p, m, \alpha)$ which equals the number of subsets $S \subseteq \{1,\ldots, p-1\}$ with the property that $\sum_{x\in S} x^m \equiv \alpha \pmod p$. We obtain a closed form expression for $N(p, m, \alpha)$. We give simple explicit formulas for $N(p, 2, \alpha)$ (which in some cases involve class numbers and fundamental units), and show that for a fixed $m$, the difference between $N(p, m, \alpha)$ and its average value $p^{-1}2^{p-1}$ is of the order of $\exp(p^{1/2})$ or less. Finally, we obtain the curious result that if $p-1$ does not divide $m$, then $N(p, m, 0) > N(p, m, \alpha)$ for all $\alpha \not\equiv 0 \pmod p$.

## 1. INTRODUCTION

Let $p$ be an odd prime, and let $F_p$ denote the field of integers modulo $p$. Let $m$ be a positive integer and let $\alpha \in F_p$. We are interested in the following problem: How many subsets $S$ of $F_p^* = F_p - \{0\}$ have the property that

$$\sum_{x\in S} x^m = \alpha \qquad (\text{in } F_p)?$$

(We allow $S$ to be void, and we set $\sum_{x\in\varnothing} x^m = 0$). Call this number $N(p, m, \alpha)$. Clearly $N(p, m, \alpha) = N(p, m', \alpha)$ if $(p-1, m) = (p-1, m')$. Hence we may assume without loss of generality that $m \mid (p-1)$. Moreover, it is also clear that

$$N(p, m, \alpha) = N(p, m, \alpha\beta^m), \qquad \alpha \in F_p, \beta \in F_p^*.$$

* Partially supported by Bell Telephone Laboratories and by N.S.F Grant No. MCS 7308445-AO4.



0022-314X/78/0102-0263$02.00/0

Hence for given $p$ and $m \mid (p-1)$, there are $1+m$ inequivalent values of $N(p, m, \alpha)$, viz., one for $\alpha = 0$ and one for each coset of the $m$th power residues in $F_p^*$.

Since $x^{p-1} \equiv 1 \pmod{p}$ for $x \not\equiv 0$,

$$N(p, p-1, \alpha) = \binom{p-1}{\alpha}, \qquad 0 \leqslant \alpha \leqslant p-1.$$

Similarly, if $m = (p-1)/2$, then $x^m \equiv \pm 1 \pmod{p}$ for $x \not\equiv 0 \pmod{p}$ with each value taken on exactly $m$ times. Hence if $0 \leqslant \alpha \leqslant m$, then any subset enumerated by $N(p, m, \alpha)$ corresponds uniquely to a choice of a non-negative integer $k$ and of $\alpha + k$ of the $m$ elements for which $x^m \equiv 1 \pmod{p}$, and of $m-k$ of the $m$ elements for which $x^m \equiv -1 \pmod{p}$ (the $m-k$ elements that do not belong to that subset). Hence we obtain

$$N(p, m, \pm\alpha) = \binom{p-1}{m+\alpha}, \qquad 0 \leqslant \alpha \leqslant m.$$

These two results are somewhat atypical, due to the large size of $m$ compared to $p$. For $m$ reasonably small, one might expect the values of $N(p, m, \alpha)$ for various $\alpha$ to be approximately equal; i.e., to differ from $p^{-1}2^{p-1}$ by a small error term. The main goal of this note is to explore the nature of this error term.

The case $m = 1$ has been thoroughly studied, even when $F_p$ is replaced by the ring of integers modulo $n$ for any $n > 0$. The evaluation of $N(n, 1, \alpha)$ is implicit in [3] and some references given there, and more explicit in [4]. Since for many values of $m$ the values $N(p, m, \alpha)$ regarded as a function of $\alpha$ behave exactly like $N(p, 1, \alpha)$, we give a direct evaluation of this last quantity. If $S$ is any nonvoid subset of $F_p^*$ and $\alpha \in F_p$, then there is clearly a unique $\beta \in F_p$ such that $\sum_{x \in S}(x + \beta) = \alpha$. Hence any given $\alpha \in F_p$ appears equally often as a sum of the elements of the $2^p - 2$ proper subsets of $F_p$, viz., $(2^p - p)/p$ times. The $2^p - 2$ proper subsets of $F_p$ come in pairs $(S, T)$ where $0 \notin S$ and $T = S \cup \{0\}$, except that the subsets $\{0\}$ and $F_p^*$ remain unpaired. In each pair $(S, T)$ the sets $S$ and $T$ have the same element sum, while $\{0\}$ and $F_p^*$ also have the same element sum 0 (this is where it is necessary to assume $p$ is odd). Hence each $\alpha \in F_p$ appears $(2^{p-1} - 1)/p$ times as a sum of the elements of the $2^{p-1} - 1$ nonvoid subsets of $F_p^*$. It follows that

$$N(p, 1, \alpha) = \begin{cases} p^{-1}(2^{p-1} - 1) & \text{if } \alpha \neq 0, \\ p^{-1}(2^{p-1} + p - 1) & \text{if } \alpha = 0, \end{cases} \tag{1}$$

since the contribution of the null set is by definition zero.

This note proves several new results about the numbers $N(p, m, \alpha)$. First (Lemma 2.1) an explicit formula, suitable for numerical computation, is found for $N(p, m, \alpha)$ in terms of roots of unity. This formula is then used to show that if 2 or $-2$ is an $m$th power residue modulo $p$, then $N(p, m, \alpha)$ has a very simple form (Theorem 3.1), and in fact equals $N(p, 1, \alpha)$, which is given by (1). In particular, this determines $N(p, 2, \alpha)$ unless $p \equiv 5 \pmod 8$. Next we express $N(p, m, \alpha)$ in terms of values of Dirichlet $L$-functions $L(s, \chi)$ at $s = 1$ (Lemmas 1.1 and 4.1). This result shows easily (Theorem 4.2) that there exists a constant $c > 0$ such that

$$| N(p, m, \alpha) - p^{-1} 2^{p-1} | < \exp(cmp^{1/2}) \log p),$$

for all $\alpha$, which justifies our claim that $N(p, m, \alpha)$ is almost equal to $p^{-1}2^{p-1}$ for small $m$. The formula involving $L(1, \chi)$, together with Dirichlet's class number formula, also allows us to determine $N(p, 2, \alpha)$ explicitly in the one remaining case $p \equiv 5 \pmod 8$ (Theorem 5.1). The answer there turns out to depend on the class number and fundamental unit of $Q(p^{1/2})$. Finally, in the last section we show that $N(p, m, 0) > N(p, m, \alpha)$ for all $\alpha \in F_p^*$, provided $m < p - 1$.

Some of the results of this note can be straightforwardly extended to the case when $p$ is not assumed prime. In fact, there are at least two possible extensions; to the case where we consider all the $2^{p-1}$ subsets of $\{1,..., p - 1\}$ and to the case where we consider the $2^{\phi(p)}$ subsets of $\{k: 1 \leqslant k \leqslant p - 1, (k, p) = 1\}$. It turns out, however, that some of the generalizations break down for composite $p$. We will point out some of the differences in the text. We will not consider it for the sake of simplicity, but the most natural generalization would probably be to finite fields.

## 2. Basic Results

We now derive an expression for $N(p, m, \alpha)$ which will be a basic tool in what follows. Let $\zeta = e^{2\pi i/p}$, a primitive $p$th root of unity.

8.1 Lemma. *We have*

$$N(p, m, \alpha) = \frac{1}{p} \sum_{j=0}^{p-1} \zeta^{-\alpha j} \prod_{k=1}^{p-1} (1 + \zeta^{jk^m}). \tag{2}$$

*Proof.* Let

$$f(p, m, j) = \prod_{k=1}^{p-1} (1 + \zeta^{jk^m}), \tag{3}$$

and if $S \subset F_p^*$, let $\sigma(S) = \sum_{x \in S} x^m$. Then

$$\frac{1}{p} \sum_{j=0}^{p-1} \zeta^{-\alpha j} f(p, m, j) = \frac{1}{p} \sum_{j=0}^{p-1} \zeta^{-\alpha j} \sum_{S \subset F_p^*} \zeta^{j\sigma(S)}$$

$$= \frac{1}{p} \sum_{S \subset F_p^*} \sum_{j=0}^{p-1} \zeta^{j(\sigma(S)-\alpha)}.$$

But

$$\sum_{j=0}^{p-1} \zeta^{j(\sigma(S)-\alpha)} = \begin{cases} 0, & \text{if } \sigma(S) \neq \alpha \\ p, & \text{if } \sigma(S) = \alpha, \end{cases}$$

and the proof follows.

The above result remains true even if $p$ is composite, provided we consider all subsets of $\{1, \ldots, p-1\}$. If $p$ is composite and we consider only subsets of the integers relatively prime to $p$, then the product in (2) and (3) should be taken over only those $k$ for which $(k, p) = 1$.

## 3. The Easy Case

There is a special class of $p$ and $m$, including the case $m = 1$, for which $N(p, m, \alpha)$ behaves exactly as if $m = 1$.

3.1 Theorem. *Suppose 2 or $-2$ is an $m$th power residue modulo $p$, and assume $m \mid (p-1)$, $m < p-1$. Then*

$$N(p, m, \alpha) = \begin{cases} p^{-1}(2^{p-1} + p - 1), & \alpha = 0 \\ p^{-1}(2^{p-1} - 1), & \alpha \neq 0 \end{cases}$$

*Proof.* Let $f(p, m, j)$ be defined by (3). Suppose first that 2 is an $m$th power residue modulo $p$. Then $k^m$ and $2k^m$ range over the same elements of of $F_p^*$ as $k$ ranges over $F_p^*$. Letting all products below range from $k = 1$ to $k = p-1$, we obtain

$$f(p, m, j) = \frac{\prod(1 - \zeta^{2jk^m})}{\prod(1 - \zeta^{jk^m})} = 1, \qquad 1 \leqslant j \leqslant p-1.$$

Clearly also $f(p, m, 0) = 2^{p-1}$. Hence by Lemma 2.1,

$$N(p, m, \alpha) = \frac{1}{p}\left(2^{p-1} + \sum_{j=1}^{p-1} \zeta^{-\alpha j}\right)$$

$$= \begin{cases} \frac{1}{p}(2^{p-1} + p - 1), & \alpha = 0 \\ \frac{1}{p}(2^{p-1} - 1), & \alpha \neq 0. \end{cases}$$

Now suppose $-2$ is an $m$th power residue modulo $p$. We now write

$$f(p,m,j) = \frac{\prod \zeta^{2jk^m}(\zeta^{-2jk^m} - 1)}{\prod (1 - \zeta^{jk^m})}$$

$$= \zeta^{2j(1^m+2^m+\cdots+(p-1)^m)} \frac{\prod (1 - \zeta^{-2jk^m})}{\prod (1 - \zeta^{jk^m})}$$

$$= \zeta^{2j(1^m+2^m+\cdots+(p-1)^m)}.$$

However, it is well known that $1^m + 2^m + \cdots + (p-1)^m \equiv 0 \pmod p$ whenever $m < p - 1$, as can be seen by expressing all the summands in terms of any primitive root. (Alternatively, we could use the fact that $1^m + 2^m + \cdots + x^m$ has the form $(x+1)f(x)/(m+1)!$, where $f(x)$ is a polynomial with integral coefficients.) This completes the proof.

The above analysis breaks down if $p$ is composite, since $1^m + \cdots + (p-1)^m \not\equiv 0 \pmod p$ in general for $p$ not a prime, even when there are primitive roots modulo $p$. (However, Theorem 3.1 does remain valid if $m+1$ is smaller than the least prime factor of $p$. This follows from the observation made above about the polynomial expression for $1^m + \cdots + (p-1)^m$.)

## 4. Another Expression for $N(p, m, \alpha)$

To obtain further results, we will use the Dirichlet characters $\chi$ modulo $p$, the associated $L$-functions $L(s, \chi)$ and the Gaussian sums $\tau(\chi)$[1, 2].

4.1 Lemma. *Suppose that* $m \mid p-1$, $j \not\equiv 0 \pmod p$, *and* $f(p,m,j)$ *is defined by* (3). *Let* $\chi_1, \ldots, \chi_m$ *be the* $m$ *characters modulo* $p$ *of order* $m$, *with the convention that* $\chi_1$ *is the identity character. Then*

$$f(p,m,j) = \exp\left\{ \sum_{r=2}^{m} (1 - \bar{\chi}_r(2))\, \bar{\chi}_r(j)\, \tau(\chi_r)\, L(1, \bar{\chi}_r) \right\}. \tag{5}$$

*Proof.* Taking the logarithm of (3), we obtain

$$\log f(p,m,j) = \sum_{k=1}^{p-1} \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n} \zeta^{jnk^m}$$

$$= \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n} \sum_{k=1}^{p-1} \zeta^{jnk^m}. \tag{6}$$

We next express the inner sum above in terms of the characters $\chi_1, \ldots, \chi_m$. Since $\chi_1, \ldots, \chi_m$ are the characters of the multiplicative group $F_p^*$ modulo

the multiplicative group of $m$th power residues, we have for $a \in F_p^*$ the orthogonality relation

$$\sum_{r=1}^{m} \bar{\chi}_r(a)\,\chi_r(b) = \begin{cases} m, & a = bk^m, \quad \text{some } k \in F, \\ 0, & \text{otherwise} \end{cases}$$

Hence for $a \not\equiv 0 \pmod{p}$,

$$\sum_{k=1}^{p-1} \zeta^{ak^m} = m \sum_{\substack{b \in F_p^* \\ b = ak^m \\ \text{some } k \in F_p^*}} \zeta^b = \sum_{b=1}^{p-1} \zeta^b \sum_{r=1}^{m} \bar{\chi}_r(a)\,\chi_r(b)$$

$$= \sum_{r=1}^{m} \bar{\chi}_r(a) \sum_{b=1}^{p-1} \chi_r(b)\zeta^b = \sum_{r=1}^{m} \bar{\chi}_r(a)\tau(\chi_r).$$

Combining this with (5) we obtain

$$\log f(p, m, j) = \sum_{\substack{n=1 \\ p \mid n}}^{\infty} \frac{(-1)^{n-1}}{n}(p-1)$$

$$+ \sum_{\substack{n=1 \\ p \nmid n}}^{\infty} \frac{(-1)^{n-1}}{n} \sum_{r=1}^{m} \bar{\chi}_r(jn)\,\tau(\chi_r).$$

In the second sum on the right we have $\chi_1(jn) = \chi_1(j)\,\chi_1(n) = 1$ for $(j, p) = 1$, $(n, p) = 1$, and $\tau(\chi_1) = -1$, so the trivial character and the first sum over those $n$ such that $p \mid n$ together contribute

$$(p-1) \sum_{\substack{n=1 \\ p \mid n}}^{\infty} \frac{(-1)^{n-1}}{n} - \sum_{\substack{n=1 \\ p \nmid n}}^{\infty} \frac{(-1)^{n-1}}{n} = p \sum_{\substack{n=1 \\ p \mid n}}^{\infty} \frac{(-1)^{n-1}}{n} - \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n}$$

$$= p \sum_{s=1}^{\infty} \frac{(-1)^{sp-1}}{sp} - \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n} = 0.$$

Therefore, since $\chi_r(s) = 0$ if $(s, p) \neq 1$, we have

$$\log f(p, m, j) = \sum_{\substack{n=1 \\ p \nmid n}} \frac{(-1)^{n-1}}{n} \sum_{r=2}^{m} \bar{\chi}_r(jn)\,\tau(\chi_r)$$

$$= \sum_{r=2}^{m} \bar{\chi}_r(j)\,\tau(\chi_r) \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n} \bar{\chi}_r(n)$$

$$= \sum_{r=2}^{m} \bar{\chi}_r(j)\,\tau(\chi_r)(1 - \bar{\chi}_r(2)) \sum_{n=1}^{\infty} \frac{\bar{\chi}_r(n)}{n},$$

which completes the proof.

Our next result follws easily from the above lemma.

4.2 THEOREM. *There is a constant $c > 0$ such that for any $p$, $m$, and $\alpha$,*

$$\left| N(p, m, \alpha) - \frac{1}{p} 2^{p-1} \right| < \exp\{cm\ p^{1/2}\ \log p\}.$$

*Proof.* It is well known [1, 2] that $|\tau(\chi)| = p^{1/2}$ for any nonidentity character mod $p$, and that [2, p. 110] $|L(1, \chi)| < c' \log p$ for some constant $c' > 0$. Hence for $j \not\equiv 0 \pmod{p}$, Lemma 4.1 yields

$$|f(p, m, j)| \leqslant \exp\{2c'(m-1)\, p^{1/2} \log p\},$$

which together with Lemma 2.1 proves the theorem.

## 5. THE CASE $m = 2$

If 2 or $-2$ is a quadratic residue modulo $p$, then $N(p, 2, \alpha)$ is given by Theorem 3.1. However, the only odd primes $p$ which have neither 2 nor $-2$ as a quadratic residue are those with $p \equiv 5 \pmod 8$. In this case we can evaluate $N(p, 2, \alpha)$ by using Lemma 4.1 and Dirichlet's class number formula.

5.1 THEOREM. *Let $p \equiv 5 \pmod 8$, and let $h$ be the class number of $Q(p^{1/2})$, and $\epsilon > 1$ the fundamental unit of $Q(p^{1/2})$. Then*

$$N(p, 2, \alpha) = \begin{cases} \dfrac{1}{p}\left[2^{p-1} + \dfrac{p-1}{2}\left(\epsilon^{4h} + \epsilon^{-4h}\right)\right], & \alpha = 0 \\ \dfrac{1}{p}\left[2^{p-1} + \epsilon^{4h}\left(\dfrac{-1+p^{1/2}}{2}\right) + \epsilon^{-4h}\left(\dfrac{-1-p^{1/2}}{2}\right)\right], & \text{if } \left(\dfrac{\alpha}{p}\right) = 1 \\ \dfrac{1}{p}\left[2^{p-1} - \epsilon^{4h}\left(\dfrac{1+p^{1/2}}{2}\right) - \epsilon^{-4h}\left(\dfrac{1-p^{1/2}}{2}\right)\right], & \text{if } \left(\dfrac{\alpha}{p}\right) = -1. \end{cases}$$

*Proof.* Since $m = 2$, we have only one term in the sum on the right side of (5), namely the one corresponding to the Legendre symbol $\chi_2(j) = (j/p)$. Also, $\tau(\chi_2) = p^{1/2}$ and by Dirichlet's class number formula [2, Chap. 6]

$$L(1, \chi_1) = \frac{2h \log \epsilon}{p^{1/2}}.$$

Hence

$$f(p, m, j) = \exp\{4(j/p)h \log \epsilon\} = \begin{cases} \epsilon^{4h}, & \text{if } (j/p) = 1, \\ \epsilon^{-4h}, & \text{if } (j/p) = -1. \end{cases}$$

Now apply Lemma 2.1. If $\alpha = 0$, we get

$$N(p, 2, 0) = \frac{1}{p}\left(2^{p-1} + \sum f(p, 2, j)\right).$$

Exactly half the elements of $F_p^*$ are quadratic residues and half nonresidues, so the theorem follows for $\alpha = 0$.

If $\alpha$ is a quadratic residue, say $\alpha = +1$, we obtain

$$N(p, 2, \alpha) = \frac{1}{p}\left(2^{p-1} + \sum \zeta^{-j} f(p, 2, j)\right)$$

$$= \frac{1}{p}\left(2^{p-1} + \epsilon^{4h} \sum_{(j/p)=1} \zeta^j + \epsilon^{-4h} \sum_{(j/p)=-1} \zeta^j\right).$$

It is an immediate consequence of the Gauss sum evaluation $\sum (j/p)\, \zeta^j = p^{1/2}$, together with $\sum_{j=1}^{p-1} \zeta^j = -1$, that

$$\sum_{(j/p)=1} \zeta^j = \frac{-1 + p^{1/2}}{2}, \qquad \sum_{(j/p)=-1} \zeta^j = \frac{-1 - p^{1/2}}{2}.$$

From this the theorem follows for $(\alpha/p) = 1$.

The case $(\alpha/p) = -1$ is done in exact analogy to the previous case, so the proof is complete.

The Siegel formula on the class number implies that $\log(h \log \epsilon) \sim \frac{1}{2} \log p$ as $p \to \infty$, $p \equiv 5 \pmod 8$. Hence $\epsilon^{4h}$ is roughly of the order $e^{p^{1/2}}$, so that for instance $N(p, 2, 0)$ exceeds the "expected" value $2^{p-1}/p$ by about $e^{p^{1/2}}$ when $p \equiv 5 \pmod 8$. In particular, this shows that the bound of Theorem 4.2 is not far from best possible. It is also interesting to note that if $p \equiv 5 \pmod 8$, $(\alpha/p) = 1$, $(\beta/p) = -1$, then

$$N(p, 2, \alpha) - N(p, 2, \beta) = \frac{1}{p^{1/2}} (\epsilon^{4h} - \epsilon^{-4h}).$$

The fact that the left-hand side is positive is essentially equivalent to the relatively deep result that the Gauss sum $\sum (j/p)\, \zeta^j$ is positive.

It is interesting to compare the proof of Theorem 3.1 with Lemma 4.1. The crucial step in the proof of Theorem 3.1 was the proof that $f(p, m, j) = 1$ for $j \not\equiv 0 \pmod p$, if either 2 or $-2$ is an $m$th power residue modulo $p$. If 2 is an $m$th power residue, this also follows easily from Lemma 4.1, since then $\bar{\chi}_r(2) = 1$ for all the characters $\chi_1, \ldots, \chi_m$. If $-2$ is an $m$th power residue, however, this is not so simple. For example, if $p \equiv 3 \pmod 8$ and $m = 2$, the $f(p, 2, j) = 1$ is equivalent to proving that

$$2ip^{1/2} L(1, \chi_2) = 2\pi i \cdot l$$

for some integer $l$ (since $\tau(\chi_2) = ip^{1/2}$). In fact Dirichlet's class number formulas show that $l$ is the class number of the field $Q((-p)^{1/2})$.

## 6. The Maximum Value

Given $p$ and $m$, we wish to show that $N(p, m, \alpha)$ is maximized at $\alpha = 0$. This is an immediate consequence of the next lemma.

6.1 Lemma. *Suppose* $m \mid (p-1)$ *and* $m \neq p-1$. *Then* $f(p, m, j)$ *is a positive real number.*

*Proof. Case* 1. $m$ is odd. In this case the $p-1$ factors of $\prod(1+\zeta^{jk^m})$ can be divided into $(p-1)/2$ pairs of the form $(1+\zeta^{jk^m})\times(1+\zeta^{-jk^m})>0$.

*Case* 2. $m$ is even. Let $r = (p-1)/2$. Then

$$f(p, m, j) = \prod_1^r (1+\zeta^{jk^m})^2,$$

so it suffices to show that $A = \prod_1^r (1+\zeta^{jk^m})$ is real. Its complex conjugate is given by

$$\bar{A} = \prod_1^r (1+\zeta^{-jk^m}) = \prod_1^r \zeta^{-jk^m}(1+\zeta^{jk^m}) = \zeta^t A,$$

where $t = -j(1^m + 2^m + \cdots + r^m)$. Since $m$ is even we have $2t = -j(1^m + 2^m + \cdots + (p-1)^m) \pmod p$, so just as in the proof of Theorem 3.1 we conclude $t \equiv 0 \pmod p$ if $m \neq p-1$. Hence $A = \bar{A}$, and the lemma follows.

6.2 Theorem. *Suppose* $m \mid (p-1)$, $m \neq p-1$, *and* $\alpha \in F_p{}^*$. *Then* $N(p, m, 0) > N(p, m, \alpha)$.

*Proof.* By Lemmas 2.1 and 6.1,

$$N(p, m, \alpha) = \frac{1}{p}\left|\sum_{j=0}^{p-1} \zeta^{-\alpha j} f(p, m, j)\right|$$

$$\leqslant \frac{1}{p}\sum_{j=0}^{p-1} f(p, m, j) = N(p, m, 0).$$

Equality holds if and only if $|\zeta^{-\alpha j}| = \zeta^{-\alpha j}$ for all $j$, which is impossible if $\alpha \in F_p{}^*$. This completes the proof.

Theorem 6.2 is false for composite $p$ (whether we sum over all integers or only those relatively prime to $p$), as is shown by the example $p = 21$, $m = 2$. The reason that the proof breaks down is again the fact that $1^m + \cdots + (p-1)^m \not\equiv 0 \pmod{p}$ in general if $p$ is not prime.

## REFERENCES

1. Z. I. BOREVICH AND I. R. SHAFAREVICH, "Number Theory," Academic Press, New York/London, 1966.
2. H. DAVENPORT, "Multiplicative Number Theory," Markham, Chicago, 1967.
3. C. A. NICOL, Linear congruences and the Von Sterneck function, *Duke Math. J.* **26** (1959), 193–197.
4. R. STANLEY AND M. F. YODER, "A Study of Varshamov Codes for Asymmetric Channels," JPL Technical Report 32-1526, Deep Space Network, Vol. XIV, pp. 117–123, 1972.

*Printed in Belgium*