Pacific Journal of Mathematics

FACTORIZATION OF A SPECIAL POLYNOMIAL OVER A FINITE FIELD

L. Carlitz

Vol. 32, No. 3 March 1970

PACIFIC JOURNAL OF MATHEMATICS
Vol. 32, No. 3, 1970

FACTORIZATION OF A SPECIAL POLYNOMIAL OVER A FINITE FIELD

L. CARLITZ

Let $q = p^z$, where p is a prime and $z \geqq 1$, and put $r = q^n$, $n \geqq 1$. Consider the polynomial

$$F(x) = x^{2r+1} + x^{r-1} + 1 .$$

Mills and Zierler proved that, for $q = 2$, the degree of every irreducible factor of $F(x)$ over $GF(2)$ divides either $2n$ or $3n$. We shall show that, for arbitrary q, the degree of every irreducible factor of $F(x)$ over $GF(q)$ divides either $2n$ or $3n$.

We shall follow the notation of Mills and Zierler [1]. Put

$$K = GF(r) , \qquad L = GF(r^2) , \qquad M = GF(r^3) . \tag{1.1}$$

The identity

$$(x^{(2r+1)r} + x^{(r-1)r} + 1) - x^{r^2-r}(x^{2r+1} + x^{r-1} + 1) \\ = (x^{r^2-1} - 1)(x^{r^2+r+1} - 1)$$

is easily verified. Since

$$(x^{2r+1} + x^{r-1} + 1)^r = x^{(2r+1)r} + x^{(r-1)r} + 1 ,$$

it is clear that

$$F^r(x) - x^{r^2-r}F(x) = (x^{r^2-1} - 1)(x^{r^2+r+1} - 1) . \tag{1.2}$$

Let $F(\alpha) = 0$, where α lies in some finite extension of $GF(q)$. Then by (1.2)

$$(\alpha^{r^2-1} - 1)(\alpha^{r^2+r+1} - 1) ,$$

so that either

$$\alpha^{r^2-1} - 1 = 0 \tag{1.3}$$

or

$$\alpha^{r^2+r+1} - 1 = 0 . \tag{1.4}$$

Clearly (1.4) implies

$$\alpha^{r^3-1} - 1 = 0 .$$

Hence α lies in either L or M.

Assume $\alpha \in K$. Then $\alpha^r = \alpha$, so that $F(\alpha) = 0$ reduces to

$$(1.5) \qquad \alpha^3 + 2 = 0 .$$

There are now several possibilities. First the case $p = 2$ can be ruled out since $\alpha \neq 0$. Next if $p = 3$, (1.5) reduces to $\alpha^3 = 1$, so that $\alpha = 1$. If $p > 3$ and $r \equiv 2 \pmod 3$ then again α is uniquely determined by (1.5) and is in $GF(p)$. If $p > 3$, $p \equiv 2 \pmod 3$ but $r \equiv 1 \pmod 3$, then $\alpha \in K$ if and only if

$$(1.6) \qquad (-2)^{(r-1)/3} \equiv 1 \pmod p .$$

Since $p^2 - 1 \mid r - 1$, it is clear that this condition is satisfied; hence there are three distinct values of $\alpha \in K$ that satisfy (1.5). Finally if $p \equiv 1 \pmod 3$, (1.5) will be satisfied with $\alpha \in K$ if and only if (1.6) holds and again there are three distinct values of α.

There is also a possibility that $F(x)$ has multiple roots when $p > 2$. Since

$$F'(x) = (2r + 1)x^{2r} + (r - 1)x^{r-2} = x^{2r} - x^{r-2} ,$$

it follows that a multiple root must satisfy

$$(1.7) \qquad \alpha^{r+2} = 1 .$$

Then

$$0 = \alpha^3 F(\alpha) = \alpha^{2r+4} + \alpha^{r+2} + \alpha^3 ,$$

so that $\alpha^3 + 2 = 0$. On the other hand, combining (1.7) with either (1.3) or (1.4) gives $\alpha^3 = 1$. Hence $p = 3, \alpha = 1$. Since $F''(1) = 2$ the multiplicity is 2.

To sum up we state the following two theorems.

THEOREM 1. *The degree of every irreducible factor of*

$$F(x) = x^{2r+1} + x^{r-1} + 1$$

over $GF(q)$ divides either $2n$ or $3n$.

THEOREM 2. *The only possible irreducible factors of $F(x)$ of degree dividing n are determined as follows*:

(i) $p = 3$, $x - 1$,

(ii) $p > 3$, $r \equiv 2 \pmod 3$, *linear factor*,

(iii) $p > 3$, $p \equiv 2 \pmod 3$, $r \equiv 1 \pmod 3$, $x^3 + 2$,

(iv) $p \equiv 1 \pmod 3$, $(-2)^{(r-1)/3} \equiv 1 \pmod p$, $x^3 + 2$,

(v) $p \equiv 1 \pmod 3$, $(-2)^{(r-1)/3} \not\equiv 1 \pmod p$, 1.

$F(x)$ has multiple roots if and only if $p = 3$; when $p = 3, \alpha = 1$ is a root of multiplicity 2.

Let $F_0(x)$ denote the product of the irreducible divisors of $F(x)$ over $GF(q)$ of degree dividing n and put $f_0 = \deg F_0(x)$. Then Theorem 2 implies

THEOREM 3. *We have*
(i) $f_0 = 2$,
(ii) $f_0 = 1$,
(iii) $f_0 = 3$,
(iv) $f_0 = 3$,
(v) $f_0 = 0$,
where the cases (i), $\cdots$, (v) *have the same meaning as in Theorem* 2. *When* $p = 2, f_0 = 0$.

2. If α denotes a root of $F(x)$, put

$$\beta = \alpha^{2r+1} . \tag{2.1}$$

Thus

$$\beta + \alpha^{r-1} + 1 = 0 ,$$

so that

$$(\beta + 1)^{2r+1} + \beta^{r-1} = 0 . \tag{2.2}$$

Expanding the left member of (2.2) we get

$$\beta^{2r+1} + \beta^{2r} + 2\beta^{r+1} + 2\beta^{r} + \beta^{r-1} + \beta + 1 = 0 ;$$

this is the same as

$$(\beta^{r} + \beta^{r-1} + 1)(\beta^{r+1} + \beta + 1) = 0 . \tag{2.3}$$

Now define

$$G(x) = (x^{r} + x^{r-1} + 1)(x^{r+1} + x + 1) .$$

It follows that if α is a root of $F(x)$, then α^{2r+1} is a root of $G(x)$.

As in [1], put

$$G_1(x) = x^{r} + x^{r-1} + 1 , \qquad G_2(x) = x^{r+1} + x + 1 ,$$

so that

$$G(x) = G_1(x)G_2(x) .$$

Also it is convenient to put

$$H(x) = x^{r} + x + 1 .$$

The roots of $H(x)$ are the inverse of the roots of $G_1(x)$.

If $H(\beta) = 0$ then

$$\beta^r = -\beta - 1 , \qquad \beta^{r^2} = -\beta^r - 1 = \beta ,$$

so that $\beta \in L$. If we assume $\beta \in K$, so that $\beta^r = \beta$, it follows that $2\beta + 1 = 0$. Thus for $p > 2$, $H(x)$ has a unique root in K (indeed in $GF(p)$). Since $H'(\beta) = 1$ it is clear that $H(x)$ has no multiple root. Thus, except for the root -2, all the roots of $G_1(x)$ lie in L and not in K.

Next if $G_2(\beta) = 0$ we have

$$\beta^{r+1} = -\beta - 1 ,$$

so that

$$\beta^{r^2+r+1} = -\beta(\beta + 1) = -\beta^{r+1} - \beta = 1 .$$

Hence $\beta^{r^3-1} = 1$, so that $\beta \in M$. If we assume $\beta \in K$ we get

$$\beta^2 + \beta + 1 = 0 . \tag{2.4}$$

This equation is solvable in K if and only if $p = 3$ or $r \equiv 1 \pmod 3$. Thus, except for these cases, the roots of $G_2(x)$ lie in M and not in K. Since

$$G_2'(x) = x^r + 1 = (x + 1)^r ,$$

it follows that $G_2(x)$ has no multiple roots.

This proves

LEMMA 1. *Except for the root -2 when $p > 2$, all the roots of $G_1(x)$ lie in L and not in K. Except for the root 1 when $p = 3$, all the roots of $G_2(x)$ lie in M and not in K.*

We shall now prove

LEMMA 2. *Let α be a root of $F(x)$ and put $\beta = \alpha^{2r+1}$, so that β is a root of $G(x)$. If β is a root of $G_1(x)$, then $\alpha \in L$; if β is a root of $G_2(x)$, then $\alpha^{r^2+r+1} = 1$ so that $\alpha \in M$.*

Proof. By hypothesis

$$0 = F(\alpha) = \beta + \alpha^{r-1} + 1 ,$$

so that

$$\beta = -\alpha^{r-1} - 1 . \tag{2.5}$$

Assume first that $G_1(\beta) = 0$. Then

$$1 = -\beta^{r-1}(\beta + 1) = \alpha^{(2r+1)(r-1)} \cdot \alpha^{r-1} = \alpha^{2r^2-2} ,$$

so that

$$\alpha^{2(r^2-1)} = 1$$

and $\alpha^2 \in L$. But since either $\alpha \in L$ or $\alpha \in M$ it follows that $\alpha \in L$.

Next let $G_2(\beta) = 0$. Then by (2.5)

$$\alpha^{r-1} = -\beta - 1 = \beta^{r+1} = \beta^{(r+1)(2r+1)} ,$$

which gives

$$\alpha^{2(r^2+r+1)} = 1 . \tag{2.6}$$

This implies $\alpha^2 \in M$. If $\alpha \in L$, (2.6) reduces to $\alpha^{2r+4} = 1$; this in turn gives

$$\beta^2 = \alpha^{4r+2} = 1 ,$$

so that $B = \pm 1$. Since $G_2(\beta) = 0$ we must have $p = 3, \beta = 1$.

3. By Theorem 1 we have

$$F(x) = F_1(x)F_2(x)/F_0(x) \tag{3.1}$$

where every root of $F_1(x)$ is in L, every root of $F_2(x)$ is in M, every root of $F_0(x)$ is in K.

We shall now prove

LEMMA 3. *A number $\alpha \in L$ is a root of $F_1(x)$ if and only if $\beta = \alpha^{2r+1}$ is a root of $G_1(x)$.*

Proof. By Lemma 2, if α is a root of $F_1(x)$, then β is a root of $G_1(x)$. Let $\alpha \in L$, $\beta = \alpha^{2r+1}$, $G_1(\beta) = 0$. Then since $\alpha^{r^2-1} = 1$ it follows that

$$(\alpha\beta)^{r-1} = (\alpha^{2r+2})^{r-1} = \alpha^{2(r^2-1)} = 1 .$$

Consequently

$$\begin{aligned}\beta^{r-1}F(\alpha) &= \beta^{r-1}(\beta + \alpha^{r-1} + 1)\\ &= \beta^r + \beta^{r-1} + (\alpha\beta)^{r-1}\\ &= \beta^r + \beta^{r-1} + 1\\ &= G_1(\beta) = 0 ,\end{aligned}$$

so that $F(\alpha) = 0$.

LEMMA 4. *Let α be an element of M such that $\alpha^{r^2+r+1} = 1$. Then α is a root of $F_2(x)$ if and only if $\beta = \alpha^{2r+1}$ is a root of $G_2(x)$.*

Proof. By Lemma 2, if α is a root of $F_2(x)$, then β is a root of $G_2(x)$. Let $\alpha \in M$, $\alpha^{r^2+r+1} = 1$, $\beta = \alpha^{2r+1}$, $G_2(\beta) = 0$. Since

$$\beta^{r+1} = \alpha^{(r+1)(2r+1)} = \alpha^{2r^2+3r+1} = \alpha^{r-1} ,$$

we get

$$0 = G_2(\beta) = \beta^{r+1} + \beta + 1 = \alpha^{2r+1} + \alpha^{r-1} + 1 = F(\alpha) ,$$

so that $F(\alpha) = 0$.

LEMMA 5. *Let β be a nonzero element of L and let $R(\beta)$ denote the number of elements α in L such that $\alpha^{2r+1} = \beta$. Then*

$$R(\beta) = \begin{cases} 1 & (r \equiv 0, 2 \pmod 3) \\ 3 & (r \equiv 1 \pmod 3),\ \beta = \gamma^3,\ \gamma \in L) \\ 0 & (\text{otherwise}) . \end{cases} \tag{3.2}$$

Proof. Any common divisor of $2r + 1$ and $r^2 - 1$ must divide

$$(2r - 1)(2r + 1) - 4(r^2 - 1) = 3 .$$

If $r \equiv 0, 2 \pmod 3$ then $2r + 1 \equiv 1, 2 \pmod 3$, so that $(2r + 1, r^2 - 1) = 1$. It follows that the equation $\alpha^{2r+1} = \beta$ has a unique solution $\alpha \in L$. If $r \equiv 1 \pmod 3$ we have $(2r + 1, r^2 - 1) = 3$; thus the equation $\alpha^{2r+1} = \beta$ is insolvable in L if and only if $\beta = \gamma^3, \gamma \in L$. If $\beta = \gamma^3, \gamma \in L$, there are exactly three solutions; otherwise there are none.

If $r \equiv 0, 2 \pmod 3$ it follows at once from Lemmas 3 and 5 that there is a one-to-one correspondence between the roots of $F_1(x)$ and of $G_1(x)$. We may therefore state the following.

THEOREM 4. *Let $r \equiv 0, 2 \pmod 3$. Then the degree of $F_1(x)$ is equal to r.*

If we put $f_1 = \deg F_1(x), f_2 = \deg F_2(x), f_0 = \deg F_0(x)$, then by (3.1) we have

$$f_0 + 2r + 1 = f_1 + f_2 . \tag{3.3}$$

Thus for $r \equiv 0, 2 \pmod 3), f_2$ can be computed by means of (3.3) and Theorem 3.

4. We shall now determine f_1 when $r \equiv 1 \pmod 3$. By Lemmas 3 and 5, f_1 is three times the number of roots of $G_1(x)$ that are cubes

in L. Then, if as above

$$H(x) = x^r + x + 1 ,$$

f_1 is three times the number of roots of $H(x)$ that are cubes in L.

Put $\lambda = \beta^{r+1}$, where $H(\beta) = 0$. Since $\beta^{r^2} = \beta$, it follows that $\lambda^r = \beta^{r^2+r} = \lambda$, so that $\lambda \in K$. In the next place λ is a cube in K if and only if β is a cube in L. To see this let γ denote a primitive root of L. Then $\beta = \gamma^t$, where t is some integer. If β is a cube in L then $t = 3u$, where u is an integer. Thus

$$\lambda = \beta^{r+1} = \gamma^{3u(r+1)} .$$

Since $\gamma^{r+1} \in K$, it follows that λ is a cube in K. To prove the converse, it is clear first that $\lambda = \gamma^{a(r+1)}$, where a is an integer. If λ is a cube in K it follows that $a = 3b$, where b is an integer. Thus $\lambda = \beta^{r+1}$ becomes

$$\gamma^{3b(r+1)} = \gamma^{t(r+1)} ,$$

so that

$$3b(r + 1) \equiv t(r + 1) \pmod{r^2 - 1} .$$

This implies

$$3b \equiv t \pmod{r - 1} .$$

Since $r \equiv 1 \pmod 3$ we conclude that $3/t$.

The relation $\lambda = \beta^{r+1}$, where $H(\beta) = 0$, is equivalent to

$$\beta^2 + \beta + \lambda = 0 . \tag{4.1}$$

We have seen above that, except for $\beta = -1/2$, all the roots of $H(\beta) = 0$, are in L and not in K (of course this case occurs only when $p > 2$). Moreover $\beta = -1/2, \lambda = 1/4$ do indeed satisfy (4.1). Also 2 is a cube in L if and only if it is a cube in K, that is, if and only if

$$2^{(r-1)/3} \equiv 1 \pmod p . \tag{4.2}$$

Thus aside from the exceptional case just described we must determine the number of cubes of K that are not of the form $\tau(\tau + 1)$ with τ in K (for convenience we replace λ in (4.1) by its negative). We denote this number by N. If N_0 denotes the number of nonzero cubes of K that are of the form $\tau(\tau + 1)$ with τ in K, it is clear that

$$N + N_0 = \frac{1}{3}(r - 1) . \tag{4.3}$$

As for f_1, we have

(4.4) $$f_1 = 6N + 3E\,,$$

where $E = 1$ when (4.2) is satisfied and $E = 0$ otherwise. The coefficient 6 occurs because for given $\lambda \neq 1/4$ there are two distinct values of β; however when $\lambda = 1/4$ there is a single value of β and hence the coefficient 3.

It remains therefore to evaluate N_0. Clearly $6N_0$ is equal to the number of pairs $x, y \in K$ such that

(4.5) $$x^2 + x = y^3 \neq 0\,.$$

Assume first that $p > 2$. Then (4.5) is equivalent to

(4.6) $$z^2 = 4y^3 + 1\,, \qquad y \neq 0\,.$$

Let $\psi(a)$ denote the quadratic character for K, that is

$$\psi(a) = \begin{cases} +1 & (a = b^2 \neq 0,\, b \in K) \\ 0 & (a = 0) \\ -1 & (\text{otherwise})\,. \end{cases}$$

Then the number of solutions of (4.6) is equal to

$$\sum_{\substack{y \in K \\ y \neq 0}} \{1 + \psi(4y^3 + 1)\}\,,$$

so that

(4.7) $$6N_0 = r - 2 + \sum_{y \in K} \psi(4y^3 + 1)\,,$$

where now the summation is over all $y \in K$.

Put

$$J(a) = \sum_{x = K} \psi(x^3 + a) \qquad (a \in K)\,.$$

Then clearly

$$J(ac^3) = \psi(c)J(a) \qquad (c \neq 0)\,,$$

so that

(4.8) $$J^2(ac^3) = J^2(c) \qquad (c \neq 0)\,.$$

$$\begin{aligned} \sum_a J^2(a) &= \sum_{x,y} \sum_a \psi((x^3 + a)(y^3 + a)) \\ &= \sum_{x^2 = y^3} (r - 1) - \sum_{x^3 \neq y^3} 1 \\ &= r \sum_{x^3 = y^3} 1 - \sum_{x,y} 1 \\ &= r(3r - 2) - r^2 \\ &= 2r(r - 1)\,, \end{aligned}$$

so that

$$\sum_{a} J^2(a) = 2r(r-1) \; . \tag{4.9}$$

Let γ denote a fixed primitive root of K. Then by (4.8) and (4.9), since $J(0) = 0$,

$$J^2(1) + J^2(\gamma^2) + J^2(\gamma^4) = 6r \; . \tag{4.10}$$

On the other hand, since

$$\sum_{c} J(c^2) = \sum_{x} \sum_{c} \psi(x^3 + c^2) = r - 1 - \sum_{x \neq 0} 1 = 0 \; ,$$

it follows that

$$J(1) + J(\gamma^2) + J(\gamma^4) = 0 \; . \tag{4.11}$$

Combining (4.11) with (4.10), we get

$$J^2(1) + J(1)J(\gamma^2) + J^2(\gamma^2) = 3r \; . \tag{4.12}$$

It is easily seen that $J(1)$ is an even integer while $J(\gamma^2)$, $J(\gamma^4)$ are odd. Thus (4.12) implies

$$r = A^2 + 3B^2 \; , \tag{4.13}$$

where A, B are integers defined by

$$A = \frac{1}{2}J(1) \; , \qquad B = \frac{1}{6}[J(1) + 2J(\gamma^2)] \; . \tag{4.14}$$

It follows from the definition that

$$J(1) \equiv 1 \pmod 3 \; . \tag{4.15}$$

Hence, by (4.11) and (4.12),

$$J(1) \equiv J(\gamma^2) \equiv J(\gamma^4) \equiv 1 \pmod 3 \; . \tag{4.16}$$

If $p \equiv 2 \pmod 3$ it is clear from (4.13) that $A = \pm r^{1/2}$, $B = 0$. Thus, by (4.11), (4.14) and (4.16),

$$J(1) = \pm 2r^{1/2} \equiv 1 \pmod 3 \tag{4.17}$$

and

$$J(\gamma^2) = J(\gamma^4) = -\frac{1}{2}J(1) \; . \tag{4.18}$$

For $p \equiv 1 \pmod 3$, on the other hand, we have the congruence

$$J(1) \equiv -\binom{3m}{2m}^{nz} \pmod p \; ,$$

where $p = 6m + 1$. Thus $J(1) \neq 0 \pmod p$. Hence A^2, B^2 in (4.13) are uniquely determined. Then making use of (4.16), $J(1)$, $J(\gamma^2)$, $J(\gamma^4)$ are uniquely determined.

Returning to (4.7), we have

$$6N_0 = r - 2 + \psi(2)J(2) . \tag{4.19}$$

Thus, by (4.3) and (4.4), we get

$$f_1 = r - \psi(2)J(2) - 3E . \tag{4.20}$$

We may state

THEOREM 5. *Let $p > 2$, $r \equiv 1 \pmod 3$. Then the degree of $F_1(x)$ is determined by (4.20), where $J(2)$ is uniquely determined by (4.13), (4.16), (4.17) and (4.18); $E = 1$ when*

$$2^{(r-1)/3} \equiv 1 \pmod p$$

and $E = 0$ otherwise.

5. When $p = 2$ we have, as above, $f_1 = 6N$ and

$$N + N_0 = \frac{1}{3}(r - 1) ;$$

$6N_0$ is equal to the number of pairs $x, y \in K$ such that

$$x^2 + x = y^3 \neq 0 . \tag{5.1}$$

Now for $a \in K$ put

$$t(a) = a + a^2 + a^{2^2} + \cdots + a^{2^{nz-1}}$$

and

$$e(a) = (-1)^{t(a)} .$$

Define

$$L(a) = \sum_{x \in K} e(ax^3) . \tag{5.2}$$

It follows from (5.2) that

$$L(ac^3) = L(a) \qquad (c \neq 0) . \tag{5.3}$$

Since $e(a) = e(a^2)$ we have also

$$L(a) = L(a^2) = L(a^{-1}) \qquad (a \neq 0) . \tag{5.4}$$

It is easy to show that

$$\sum_{x \in K} e(ax) = \begin{cases} r & (a = 0) \\ 0 & (a \neq 0) . \end{cases}$$

Then

$$\begin{aligned} \sum_{a \in K} L^2(a) &= \sum_{x,y} \sum_{a} e(a(x^3 + y^3)) \\ &= r \sum_{x^3=y^3} 1 \\ &= r[1 + 3(r-1)] \\ &= r(3r-2) . \end{aligned}$$

Since $L(a) = r$, it follows that

(5.5) $$\sum_{a \neq 0} L^2(a) = 2r(r-1) .$$

Let γ denote a fixed primitive root of K. Then, by (5.3) and (5.5),

$$L^2(1) + L^2(\gamma) + L^2(\gamma^2) = 6r .$$

In view of (5.4) this reduces to

(5.6) $$L^2(1) + 2L^2(\gamma) = 6r .$$

In the next place

$$\sum_{a} L(a) = \sum_{x} \sum_{a} e(ax^3) = r ,$$

so that

$$\sum_{a \neq 0} L(a) = 0 .$$

By (5.3) and (5.4) this reduces to

(5.7) $$L(1) + 2L(\gamma) = 0 .$$

Combining (5.7) with (5.6) we get

$$L^2(\gamma) = r , \qquad L(\gamma) = \pm r^{1/2} .$$

But it is clear from the definition that

$$L(a) \equiv 1 \pmod 3$$

for all $a \in K$. Therefore

(5.8) $$L(\gamma) = L(\gamma^2) = (-2)^{nz/2}$$

and, by (5.7),

(5.9) $$L(1) = (-2)^{(nz+2)/2} .$$

We now return to (5.1). For fixed y, the number of solutions of (5.1) is equal to

$$1 + e(y^3) .$$

It follows that

$$\begin{aligned} 6N_0 &= \sum_{y \neq 0} \{1 + e(y^3)\} \\ &= r - 2 + L(1) . \end{aligned}$$

Then

$$\begin{aligned} f_1 = 6N &= 6\left[\frac{1}{3}(r-1) - N_0\right] \\ &= 2(r-1) - [r - 2 + L(1)] \\ &= r - L(1) . \end{aligned}$$

In view of (5.9) this becomes

$$f_1 = r - (-2)^{(nz+2)/2} .$$

This completes the proof of

THEOREM 6. *Let* $p = 2$, $q = 2^z$, $r = q^n$. *Then the degree of* $F_1(x)$ *is equal to*

$$2^{nz} - (-2)^{(nz+2)/2} .$$

The degree of $F_2(x)$ *is determined by*

$$f_0 + 2r + 1 = f_1 + f_2 ,$$

where $f_i = \deg F_i(x)$ *and* f_0 *is given by Theorem* 3.

We note that when $z = 1$, Theorem 6 reduces to Theorem 3 of [1].

REFERENCE

1. W. H. Mills and N. Zierler, *On a conjecture of Golomb*, Pacific J. Math. **28** (1969), 635-640.

Received July 14, 1969. Supported in part by NSF grant GP-7855.

DUKE UNIVERSITY

Mathematical papers intended for publication in the *Pacific Journal of Mathematics* should be in typed form or offset-reproduced, double spaced with large margins. Underline Greek letters in red, German in green, and script in blue. The first paragraph or two must be capable of being used separately as a synopsis of the entire paper. It should not contain references to the bibliography. Manuscripts, in duplicate if possible, may be sent to any one of the four editors. Please classify according to the scheme of Math. Rev. **36**, 1539-1546. All other communications to the editors should be addressed to the managing editor, Richard Arens, University of California, Los Angeles, California, 90024.

50 reprints are provided free for each article; additional copies may be obtained at cost in multiples of 50.

The *Pacific Journal of Mathematics* is published monthly. Effective with Volume 16 the price per volume (3 numbers) is $8.00; single issues, $3.00. Special price for current issues to individual faculty members of supporting institutions and to individual members of the American Mathematical Society: $4.00 per volume; single issues $1.50. Back numbers are available.

Subscriptions, orders for back numbers, and changes of address should be sent to Pacific Journal of Mathematics, 103 Highland Boulevard, Berkeley, California, 94708.

PUBLISHED BY PACIFIC JOURNAL OF MATHEMATICS, A NON-PROFIT CORPORATION

Printed at Kokusai Bunken Insatsusha (International Academic Printing Co., Ltd.), 7-17, Fujimi 2-chome, Chiyoda-ku, Tokyo, Japan.

Pacific Journal of Mathematics

Vol. 32, No. 3 March, 1970