PACIFIC JOURNAL OF MATHEMATICS
Vol. 28, No. 3, 1969

ON A CONJECTURE OF GOLOMB

W. H. MILLS AND NEAL ZIERLER

On the basis of empirical evidence for $n = 2, 3, 4,$ and 5 Golomb has conjectured that the degree of every irreducible factor of

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

over $GF(2)$ divides $6(n-1)$. We prove the stronger result that the degree of every irreducible factor of $F(x)$ divides either $2(n-1)$ or $3(n-1)$, but not $n-1$.

It follows from this that $F(x) = F_1(x)F_2(x)$, where the degrees of the irreducible factors of $F_1(x)$ divide $2(n-1)$, and the degrees of the irreducible factors of $F_2(x)$ divide $3(n-1)$. The polynomials $F_1(x)$ and $F_2(x)$ have a number of interesting properties that we discovered for small values of n by computer runs, and that later we were able to prove for arbitrary values of n. It is noteworthy that not only were these properties suggested by computer runs, but the central ideas of their proof were also suggested by these runs. The key lemma in our study of $F_1(x)$ and $F_2(x)$ was actually discovered for $n = 2, 4,$ and 6 by machine. It was then not difficult to prove it for arbitrary n.

1. A proof of Golomb's conjecture. In this paper all polynomials are over $GF(2)$.

Let n be an integer, $n \geqq 2$, and set $r = 2^{n-1}$. The polynomial we are interested in is

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

Set

$$K = GF(r),\ L = GF(r^2),\ M = GF(r^3) .$$

THEOREM 1. *Let α be a root of $F(x)$. Then $\alpha \notin K$ and either $\alpha \in L$ or $\alpha^{r^2+r+1} = 1$.*

Proof. Suppose α is in K. Then $\alpha^{r-1} = 1$ and

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

which is impossible. Hence α is not in K. Next we observe that

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