NOTE ON A PROBLEM OF DICKSON

L. CARLITZ

1. Let \( q = p^n \), where \( p \) is an odd prime. Let

\[
F(x) = a_0 x^k + \cdots + a_k \quad (a_i \in GF(q), a_0 \neq 0)
\]

be a polynomial of degree \( k \) such that \( F(\alpha) = \beta^2 \), where \( \beta \in GF(q) \) for all \( \alpha \in GF(q) \). The writer [1; 2] has proved the existence of a number \( N_k \) such that if \( q > N_k \) then

\[
F(x) = H^2(x) \quad (H(x) \in GF[q, x]);
\]

moreover \( N_k \) satisfies

\[
N_k \leq (k - 1)^2.
\]

If \( q = 11 \) and \( F(x) = x^5 + 4 \) it is easily verified that

\[
F(\alpha) = \begin{cases} 5 \equiv 4^2 \pmod{11} & (\alpha \equiv 11), \\ 3 \equiv 5^2 \pmod{11} & (\alpha \equiv 11). \end{cases}
\]

Clearly \( F(x) \) is not congruent \((\bmod 11)\) to the square of a polynomial.

We shall prove the following result.

**Theorem.** The number \( N_k \) satisfies

\[
N_k > 2k + 1.
\]

**Proof.** Put \( q = 2m + 1 \) and consider the polynomial

\[
F(x) = x^{(q-1)/2} + c \quad (c \in GF(q), c \neq 0).
\]

Clearly \( F(x) \) does not satisfy (1).

For \( \alpha \in GF(q) \) we define a real-valued function \( \psi(\alpha) \) by means of

\[
\psi(\alpha) = \begin{cases} 1 & (\alpha^m = 1), \\ -1 & (\alpha^m = -1), \\ 0 & (\alpha = 0). \end{cases}
\]

To prove the theorem it will suffice to show the existence of a number \( c \in GF(q) \) such that \( \psi(F(\alpha)) = 1 \) for all \( \alpha \in GF(q) \). This is equivalent to the existence of \( c \) such that

\[
\psi(c) = \psi(c + 1) = \psi(c - 1) = 1.
\]

Received by the editors November 13, 1961.

1 Supported in part by National Science Foundation grant G 16485.
Now when \( q = p \) it is known \([3, \text{p. 156}]\) that the number \( N_0(1, 1, 1) \) of incongruent \( e(\text{mod } p) \) satisfying (6) is determined by

\[
N_0(1, 1, 1) = \begin{cases} \\
\frac{1}{8}(p - 7) & (p \equiv -1 \text{ (mod 8)}), \\
\frac{1}{8}(p - 3) & (p \equiv 3 \text{ (mod 8)}), 
\end{cases}
\]

when \( p \equiv 3 \) (mod 4). When \( p \equiv 1 \) (mod 4) we have

\[
N_0(1, 1, 1) = \frac{1}{8}(p - 3 + \Phi_p) - 1 - \frac{1}{2} \left( \frac{2}{p} \right),
\]

where

\[
\Phi_p = \sum_{c=0}^{p-1} \left( \frac{c^3 - c}{p} \right);
\]

moreover

\[
| \Phi_p | \leq 2p^{1/2}.
\]

In the general case \( (q = p^n) \) it is not difficult to show that

\[
N_0(1, 1, 1) = \begin{cases} \\
\frac{1}{8}(q - 7) & (q \equiv -1 \text{ (mod 8)}), \\
\frac{1}{8}(q - 3) & (q \equiv 3 \text{ (mod 8)}), 
\end{cases}
\]

when \( q \equiv 3 \) (mod 4). When \( q \equiv 1 \) (mod 4) we have

\[
N_0(1, 1, 1) = \frac{1}{8}(q - 3 + \Phi_q) - 1 - \frac{1}{2} \psi(2),
\]

where

\[
\Phi_q = \sum_{c \in GP(q)} \psi(c^3 - c)
\]

and

\[
| \Phi_q | \leq 2q^{1/2} \quad (q \equiv 1 \text{ (mod 4)}).
\]

It follows from (7) that

\[
N_0(1, 1, 1) > 0
\]

for \( q \equiv 3 \) (mod 4), \( q > 7 \). For \( p \equiv 3 \) (mod 4) and \( n \) even (10) holds provided \( q > 15 \). Finally when \( p \equiv 1 \) (mod 4), (10) holds provided

\[
q - 15 \geq 2q^{1/2} \quad (q \equiv 1 \text{ (mod 8)}),
\]

\[
q - 7 \geq 2q^{1/2} \quad (q \equiv 5 \text{ (mod 8)}),
\]

that is, provided.
\[ q \geq 25 \quad (q \equiv 1 \pmod{8}), \]
\[ q \geq 13 \quad (q \equiv 5 \pmod{8}). \]

For the excluded small values of \( q \) we take
\[
F(x) = x^2 + 1 \quad (q = 7),
\]
\[
F(x) = x^4 + 1 \quad (q = 9),
\]
\[
F(x) = 2x^4 + 1 \quad (q = 13),
\]
\[
F(x) = 3x^8 + 1 \quad (q = 17).
\]

Since a polynomial of the form
\[
F(x) = ax^m + b \quad (a, b \in GF(q), ab \neq 0)
\]
is clearly not equal to the square of a polynomial in \( GF[q, x] \) the theorem follows.

Note that for \( q > 9 \) we have proved the existence of a polynomial of the form (11) such that
\[
F(a) = \beta^2 \quad (\beta \in GF(q), \beta \neq 0)
\]
for all \( a \in GF(q) \).

2. In certain cases, at least, the lower bound (3) can be improved. For example if \( q = 4m + 1 \) and we take
\[
F(x) = x^m + c \quad (c \in GF(q)),
\]
then for nonzero \( a \), \( a^m \) takes on one of the values \( \pm 1, \pm \varepsilon \), where \( \varepsilon^2 = -1 \). This leads to consideration of the sum
\[
S = \sum_{\varepsilon} \{ 1 + \psi(c) \} \{ 1 + \psi(c + 1) \} \{ 1 + \psi(c - 1) \}
\]
\[
\cdot \{ 1 + \psi(c + \varepsilon) \} \{ 1 + \psi(c - \varepsilon) \},
\]
where the summation is over all \( c \neq 1, -1, \varepsilon, -\varepsilon \). Using known estimates we find that \( S > 0 \) provided \( q \) exceeds a certain numerical bound (independent of \( k \)). It follows that
\[
N_k > 4k + 1
\]
at least for \( q \equiv 1 \pmod{4} \) and \( k \) sufficiently large.

REFERENCES