BOUNDS FOR EXPONENTIAL SUMS

By L. Carlitz and S. Uchiyama

1. Let $F(x) = a_0x^r + \cdots + a_r$ be a polynomial with integral coefficients and put

$$S = \sum_{u=1}^{p} e^{2\pi i F(u)/p}$$

where p is a prime. Some years ago Mordell [4; 67] noted the conjecture

$$|S| \leq (r-1)p^{\frac{1}{2}} \tag{1}$$

and remarked that it was presumably a consequence of the Riemann hypothesis proved by Weil [8] for the zeta-function of algebraic function fields. Indeed Hasse [3; 53] had indicated the connection in 1935.

In this note we wish to point out, in the first place, how (1) can be proved from Weil's result in a comparatively simple way. Since it is no more difficult, we consider the slightly more general situation in which the coefficients of $F(x)$ are numbers of the finite field $k = GF(q)$, $q = p^n$. For $\alpha \varepsilon k$, define

$$e(\alpha) = e^{2\pi i t(\alpha)/p}, \qquad t(\alpha) = \alpha + \alpha^p + \cdots + \alpha^{p^{n-1}} \tag{2}$$

and let

$$S = \sum_{\alpha \varepsilon k} e(F(\alpha)), \tag{3}$$

the summation extending over all numbers of k.

Let $K_0 = k[x]$ denote the domain of polynomials in the indeterminate x with coefficients in k. Let $P = P(x)$ denote an irreducible polynomial in K_0 of degree m. If $A = A(x)$ is an arbitrary polynomial in K_0, define $\rho(A, P)$ as the unique number of k such that

$$\rho(A, P) \equiv A + A^q + \cdots + A^{q^{m-1}} \pmod{P}. \tag{4}$$

Thus the congruence $U^q - U \equiv A \pmod{P}$ is solvable with $U \varepsilon K_0$ if and only if $\rho(A, P) = 0$. Next define

$$\lambda(A, P) = e\{\rho(A, P)\}, \tag{5}$$

with $e(\alpha)$ defined in (2). The definitions (4) and (5) are extended as follows. If M is an arbitrary polynomial in K_0, $M = P_1 \cdots P_\lambda$, put

$$\rho(A, M) = \sum_i \rho(A, P_i), \qquad \lambda(A, M) = \prod_i \lambda(A, P_i);$$

the P_i are irreducible polynomials, not necessarily distinct.

Received June 13, 1956.