105. On a Problem of Kodama Concerning the Hasse-Witt Matrix and the Distribution of Residues

By Harald NIEDERREITER
Austrian Academy of Sciences, Vienna, Austria

(Communicated by Shokichi IYANAGA, M. J. A., Nov. 12, 1987)

We consider the following problem posed by Prof. T. Kodama ([2], [3]). Let f be an odd prime and but $b=(f-1)/2$. Then the question is whether there exist an integer c coprime to f and an integer j such that the following property holds:

(A) *The least residue of $jc^n \bmod f$ is in the interval* $[1, b]$ *for all n with* $0 \leq n \leq r-1$, *where r is the multiplicative order of $c \bmod f$.*

This problem arose in connection with studies of the rank of the Hasse-Witt matrix for hyperelliptic function fields over finite fields ([1], [3], [5], [6], [7]).

We prove in this note that if c and j are such that property (A) holds, then the multiplicative order r of $c \bmod f$ must be small compared to f. In fact, we have the following explicit bound on r.

Theorem. *Let f be an odd prime and suppose there exist an integer c coprime to f and an integer j such that property* (A) *holds. Then we have*

$$r<\left(\frac{f+1}{2f}+\frac{1}{1+f^{1/2}}\left(\frac{1}{\pi}\log f+\frac{3}{4}\right)\right)^{-1}\left(\frac{1}{\pi}\log f+\frac{3}{4}\right)f^{1/2}.$$

Proof. Put $e(t)=e^{2\pi i t}$ for real t. If property (A) holds, then

$$r=\sum_{n=0}^{r-1}\sum_{h=1}^{b}\frac{1}{f}\sum_{k=0}^{f-1}e\left(\frac{k}{f}(jc^n-h)\right),$$

since the right-hand side represents the number of n, $0 \leq n \leq r-1$, such that the least residue of $jc^n \bmod f$ lies in $[1, b]$. By obvious manipulations we get

$$\begin{aligned} r&=\frac{1}{f}\sum_{k=0}^{f-1}\sum_{h=1}^{b}e\left(\frac{-kh}{f}\right)\sum_{n=0}^{r-1}e\left(\frac{kj}{f}c^n\right)\\ &=\frac{br}{f}+\frac{1}{f}\sum_{k=1}^{f-1}S_k\sum_{n=0}^{r-1}e\left(\frac{kj}{f}c^n\right)\end{aligned}$$

with

$$S_k=\sum_{h=1}^{b}e\left(\frac{-kh}{f}\right).$$

For $1 \leq k \leq f-1$ we have by [4, Theorem 8.3],

$$\left|\sum_{n=0}^{r-1}e\left(\frac{kj}{f}c^n\right)\right| \leq f^{1/2}-\frac{r}{1+f^{1/2}},$$

and a straightforward calculation yields