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 mod 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 mod 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 mod 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 mod 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

$$|S_k|=\left|e\left(\frac{k}{2f}\right)+1\right|^{-1} \qquad \text{for even } k,$$

$$|S_k|=\left|e\left(\frac{k}{2f}\right)-1\right|^{-1} \qquad \text{for odd } k.$$

Therefore

$$\frac{(f+1)r}{2f}=r-\frac{br}{f}\leq\frac{1}{f}\left(f^{1/2}-\frac{r}{1+f^{1/2}}\right)S \tag{1}$$

with

$$S=\sum_{k=1}^{f-1}|S_k|=\sum_{k=1}^{b}\left|e\left(\frac{k}{f}\right)+1\right|^{-1}+\sum_{k=0}^{b-1}\left|e\left(\frac{2k+1}{2f}\right)-1\right|^{-1}.$$

Now

$$\sum_{k=1}^{b}\left|e\left(\frac{k}{f}\right)+1\right|^{-1}=\sum_{k=1}^{b}\left|e\left(\frac{f-2k}{2f}\right)-1\right|^{-1}=\sum_{k=0}^{b-1}\left|e\left(\frac{2k+1}{2f}\right)-1\right|^{-1},$$

hence

$$S=2\sum_{k=0}^{b-1}\left|e\left(\frac{2k+1}{2f}\right)-1\right|^{-1}=\sum_{k=0}^{b-1}\operatorname{cosec}\pi\frac{2k+1}{2f}.$$

By comparing sums and integrals, we get

$$\begin{aligned}S&=\operatorname{cosec}\frac{\pi}{2f}+\sum_{k=1}^{b-1}\operatorname{cosec}\pi\frac{2k+1}{2f}\leq\operatorname{cosec}\frac{\pi}{2f}+\int_0^{b-1}\operatorname{cosec}\pi\frac{2x+1}{2f}\,dx\\ &<\operatorname{cosec}\frac{\pi}{2f}+\frac{f}{\pi}\int_{\pi/(2f)}^{\pi/2}\operatorname{cosec}t\,dt=\operatorname{cosec}\frac{\pi}{2f}+\frac{f}{\pi}\log\cot\frac{\pi}{4f}\\ &<\operatorname{cosec}\frac{\pi}{2f}+\frac{f}{\pi}\log\frac{4f}{\pi}.\end{aligned}$$

Using $\sin\pi x\geq 3x$ for $0\leq x\leq 1/6$, we obtain

$$S<\frac{1}{\pi}f\log f+\left(\frac{2}{3}+\frac{1}{\pi}\log\frac{4}{\pi}\right)f<\frac{1}{\pi}f\log f+\frac{3}{4}f.$$

From (1) and the above bound for S the desired bound for r follows immediately.

Remark 1. Our theorem implies the simpler bound

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

hence we have $r=O(f^{1/2}\log f)$ with an absolute implied constant. More generally, the method of proof shows that if for some $0<\alpha<1$ the least residue of $jc^n \bmod f$ lies in $[1,\alpha f]$ for all n with $0\leq n\leq r-1$, then $r=O((1-\alpha)^{-1}f^{1/2}\log f)$ with an absolute implied constant.

Remark 2. Property (A) cannot hold for even r since then $jc^{r/2}\equiv -j \bmod f$. The problem is trivial for $r=1$. For $r=3$ and $r=5$ examples of property (A) have been given by Nakahara [2]. This paper also contains examples of property (A) where r is of the order of magnitude $\log f$. The bound on r in our theorem can be used to limit the search for solutions of (A) when the prime f is given, or to bound f from below if r is given.

Acknowledgment. The author is grateful to Prof. T. Nakahara of Saga University for pointing out this problem.

References

[1] T. Kodama: On the rank of the Hasse-Witt matrix. Proc. Japan Acad., **60A**, 165–167 (1984).

[2] T. Nakahara: On a periodic solution of some congruences. Rep. Fac. Sci. Engrg. Saga Univ. Math., **14**, 1–5 (1986).

[3] ——: The rank of the Hasse-Witt matrix and a periodic solution of some congruences. Saga Univ. (1987) (preprint).

[4] H. Niederreiter: Quasi-Monte Carlo methods and pseudorandom numbers. Bull. Amer. Math. Soc., **84**, 957–1041 (1978).

[5] H. Stichtenoth: Die Hasse-Witt-Invariante eines Kongruenzfunktionenkörpers. Arch. Math., **33**, 357–360 (1979).

[6] T. Washio and T. Kodama: Hasse-Witt matrices of hyperelliptic function fields. Sci. Bull. Fac. Ed. Nagasaki Univ., **37**, 9–15 (1986).

[7] ——: A note on a supersingular function field. Sci. Bull. Fac. Ed. Nagasaki Univ., **37**, 17–21 (1986).