## Sergey Varbanets

Department of Computer Algebra and Discrete Mathematics, I.I. Mechnikov Odessa National University, Odessa, Ukraine
Email address: varb@sana.od.ua
Key words and phrases. Exponential sums, Kloosterman sums, pseudorandom numbers sequences

## Inversive congruential generator of the second order with a variable shift

Sergey Varbanets

Our talk is devoted to research of statistical properties of the sequences of pseudorandom numbers produced by the inversive generator of second order

$$
\begin{equation*}
y_{n+1} \equiv \frac{a}{y_{n-1} y_{n}}+b+c F(n) \quad\left(\bmod p^{m}\right) \tag{1}
\end{equation*}
$$

with $(a, p)=\left(y_{0}, p\right)=\left(y_{1}, p\right)=1, b \equiv c \equiv 0(\bmod p)$, and $F(n) \in \mathbb{Z}[n]$.
Using the recursion (1) we obtaine the representation

$$
\begin{equation*}
y_{n}=\frac{A_{0}^{(n)}+A_{1}^{(n)} y_{0}+A_{2}^{(n)} y_{1}+A_{3}^{(n)} y_{0} y_{1}}{B_{0}^{(n)}+B_{1}^{(n)} y_{0}+B_{2}^{(n)} y_{1}+B_{3}^{(n)} y_{0} y_{1}}, \tag{2}
\end{equation*}
$$

where the coefficients $A_{j}^{(n)}, B_{j}^{(n)}, j=0,1,2,3$ can be prescribe as the polynomials $f_{i}(k)$ for $n=3 k+i, i=0,1,2$.

We determinate a period length of the sequence $\left\{y_{n}\right\}$, besides this period reaches a maximum $\tau=3 p^{m-\nu_{0}-\alpha}$ if $\nu_{p}\left(y_{0} y_{1}^{2}-a\right)<\nu_{p}(b)=\alpha$.

Moreover, we prove that the sequence of pseudorandom numbers passes 3-dimensional test on the statistical independence. Obtained results are analogue of similar results for the congruential inversive pseudorandom sequences of the first order investigated in $[\mathbf{1}],[\mathbf{2}]$.

## References

1. H. Niederreiter, I. Shparlinski Exponential sums and the distribution of inversive congruential pseudorandom numbers with prime-power modulus. Acta Arith. 2000. V. 90 N. 1. P. 89-98.
2. S. Varbanets, Generalizations of Inversive Congruential Generator. Analytic and Probabilistic Methods in Number Theory, Proceedings of the Fifth International Conference in Honour of J. Kubilius, Palanga, Lithuania, 4-10 September 2011, 2012. P. 265-282.

## Contact information

## Sergey Varbanets

Department of Computer Algebra and Discrete Mathematics, I.I. Mechnikov Odessa National University, Odessa, Ukraine
Email address: varb@sana.od.ua
Key words and phrases. Congruential generators, pseudorandom numbers sequences, discrepancy

