International Journal of Pure and Applied Mathematics
Volume 103 No. 4 2015, 597-611
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
doi: http://dx.doi.org/10.12732/ijpam.v103i4.1

INVERSIVE CONGRUENTIAL GENERATOR WITH A VARIABLE SHIFT OF PSEUDORANDOM POINTS OVER THE COMPLEX PLANE

Tran The Vinh

Department of Computer Algebra and Discrete Mathematics
I.I. Mechnikov Odessa National University
St. Dvoryanskaya 2, 65026 Odessa, UKRAINE

Abstract: Consider the generator of pseudorandom points on unit square produced by the inversive congruential recursion over the ring of Gaussian integers. Study the exponential sums on sequences of these points.

AMS Subject Classification: 11K45, 11T71, 94A60, 11L07, 11T23
Key Words: pseudorandom numbers, exponential sums, Gaussian integers, inversive congruential generator

1. Introduction

Inversive congruential generator of pseudorandom numbers (PRN's) on the unit segment $[0, 1)$ of real line arose as an alternative to D. Lemer's linear generator that didn't guarantee the "unpredictability" of elements of the generated sequence. It turned out that the non-linear congruential generators of the sequence of PRN's only may provide the unpredictability of the sequence of PRN's.

We say, that the sequence of real numbers $\{x_n\}$, $x_n \in [0, 1)$, $n = 0, 1, 2, \ldots$ be the sequence of PRN's if it is generated by the determine algorithm and behaves like the sequence of implementations of random variables $\xi_0, \xi_1, \xi_2 \ldots$ that are uniformly distributed and statistically independent. Such definition

Received: January 22, 2015

of the sequence of PRN's is quiet reasonable to be apply in the modelling of stochastic processes and cryptography(for example, in forming the random key). Since every congruent sequence has a period that is not great than module of congruence, for application it is necessary to guarantee the pretty large period length. The one needs also an efficient software and hardware implementation for respective recursion.

In 1986 Eichenauer and Lehn[3] and then the Niederreiter[12][13] proposed the inversive congruential generator defined by recursion

$$y_{n+1} \equiv ay_n^{-1} + b \pmod{p},\ n = 0, 1, 2, \ldots\ (p > 2 \text{ is prime number}), \qquad (1)$$

where $y_0 \in \mathbb{Z}_p^*$, $a, b \in \mathbb{Z}$, y_n^{-1} is a solution of congruence $y_0 x \equiv 1 \pmod{p}$ if $(y_n, p) = 1$, or $y_n^{-1} = 0$ if $y_n = 0$.

Under certain conditions, the recursion (1) generates the sequence $\{y_n\}$ (and therefore the sequence $x_n = \frac{y_n}{p} \in [0, 1)$). It is clear that the sequence $\{y_n\}$ has a period $\tau \leq p$, and so for the applications it is necessary to choose a big prime number p. At the present time there are described the conditions when the period of its sequence is near to p (see, for example, Chou[1]). A big period of sequence of PRN's may be provide by recursion

$$y_{n+1} \equiv ay_n^{-1} + b \pmod{p^m}, \qquad (2)$$

where $p \geq 2$ is prime, m is natural, $a, b, y_0 \in \mathbb{Z}_{p^m}$, $(y_0, p) = 1$, y_n^{-1} is a multiplicative inverse to $y_n \pmod{p^m}$.

Generator (2) was being investigated in works of Eichenauer[8],[9], Eichenauer, Topuzoğlu[7], Huber[10], Niederreiter, Shparlinski[14]. It is clear that the generator (2) will stop work if on the certain step will such y_n, that $y_n \equiv 0 \pmod{p}$. Chou[1][2] found the conditions of existence the generator (2) and gave the description of periods for according sequences of PRN's.

In the works of Eichenauer, Lehn and Topuzoğlu[5]; Eichenauer and Niederreiter[6]; Eichenauer and Groth[4]; Kato, Wu and Yanagihara[11] there are studied the generalization of generator (2):

$$y_{n+1} \equiv ay_n^{-1} + b + xy_n \pmod{p^m} \qquad (3)$$

in case $p = 2$,
and in the works of S. Varbanets[16], P. Varbanets and S. Varbanets[17] there is considered the case of certain odd p.

Not less important for applications is to be able to build the sequences of pseudorandom points $\{z_n\}$ of unit square $0 \leq \Re(Z_n), \Im(z_n) < 1$.

The present paper is concerned with studying the distribution of points of the unit square in $\mathbb{C}$ that are generated by recursion over the ring of Gaussian integers:

$$z_{n+1} \equiv \alpha z_n^{-1} + \beta + \gamma(n) z_0 \pmod{p^m}, \tag{4}$$

where $\alpha, \beta, \gamma(n), z_0 \in \mathbb{Z}[i]$, p is prime number, $p \equiv 3 \pmod 4$.

If $\gamma(n) \neq Const$, the generator (3) is essentially call the inversive generator with a variable shift. The selection of prime number $p \equiv 3 \pmod 4$ comes from the fact that such prime rational numbers (and only one) be primes in the ring of Gaussian integers.

We construct two representations of z_n:

- in the form of polynomials in z_0 and z_0^{-1} modp^m (with coefficients depending on n) and

- in the form of polynomials in n (with coefficients depending on z_0 and z_0^{-1} modp^m).

These representations allow to obtain the non-trivial estimates of exponential sums on the elements of sequence $\{z_n\}$. And, by virtue of Turan-Erdös-Koksma inequality[15], the non-trivial estimates of exponential sums on elements of sequence $\{z_n\}$ allow to obtain the estimates for according discrepancies, and therefore, it emerges the possibility to estimate the statistical properties of $\{z_n\}$.

Notations.

$\mathbb{N}, \mathbb{Z}, G$ denote, respectively, the sets of naturals, rational integers and Gaussian integers numbers, i.e. $G = \mathbb{Z}[i] = \{a + bi \,|\, a, b \in \mathbb{Z},\ i^2 = -1\}$;

p be the prime rational number congruent with 3 modulo 4;

α, β, γ be the Gaussian integers;

$\gamma(n)$ denotes the polynomial over $G[n]$;

$\exp(x) := e^x$;

$e_{p^m}(x) := e^{2\pi i \frac{x}{p^m}}$;

$\mathbb{Z}_{p^m}$(respectively, $\mathbb{Z}_{p^m}^*$) be denote the complete (respectively, reduced) residue system modulo p^m over $\mathbb{Z}$;

G_{p^m} (respectively, $G^*_{p^m}$) be denote the complete (respectively, reduced) residue system modulo p^m over G;

$\nu_p(\alpha)$ be the nonnegative integer a such that $\alpha \equiv 0 \pmod{p^a}$, $\alpha \not\equiv 0 \pmod{p^{a+1}}$.

2. Auxiliary Results

Generator (3) we consider under conditions

$$\alpha \in G^*_{p^m},\ z_0 \in G^m_p,\ \gamma(n) = \gamma \cdot n,\ \beta, \gamma \in G_{p^m},\ \beta \equiv \gamma \equiv 0 \pmod{p}.$$

These conditions ensure the sequence $\{z_n\}$ will be not stopped and will have the big enough period.

We need the following lemmas.

Lemma 1. *For every $n = 1, 2, \ldots$, the mappings $\Phi_k : G^*_{p^m} \to G^*_{p^m}$, $k = 0, 1, \ldots$*

$$\Phi_{k+1}(z) = \alpha\Phi_k^{-1}(z) + \beta + \gamma \cdot (k+1)z,\ \Phi_0(z) = z,$$

be the permutations over $G^*_{p^m}$.

Proof. If $\gamma \equiv 0 \pmod{p^m}$, then the assertion is clear.

Let $\nu_p(\gamma) = a < m$. Then for $k = 1$ from the congruence

$$\alpha(z')^{-1} + \beta + \gamma \equiv \alpha(z'')^{-1} + \beta + \gamma \pmod{p^m}$$

it follows that $z' \equiv z'' \pmod{p}$. Let us assume that $z'' = z' + p\omega_1$. Then

$$(z'')^{-1} \equiv (z')^{-1}(1 - p\omega_1(z')^{-1}) \pmod{p^2}.$$

(here and elsewhere, all multiplicative inverses be set modulo p^m).

Then

$$\alpha(z')^{-1} + \beta + \gamma z' \equiv \alpha((z')^{-1} - p\omega_1(z')^{-2}) + \beta + \gamma(z' + p\omega_1) \pmod{p^2} \Rightarrow$$
$$\Rightarrow p\omega_1(z')^{-2} \equiv 0 \pmod{p^2} \Rightarrow \omega_1 = p\omega_2 \Rightarrow z'' = z' + p^2\omega_2 \Rightarrow$$
$$\Rightarrow (z'')^{-1} \equiv (z')^{-1} - p^2\omega_2(z')^{-2} \pmod{p^3}.$$

Now, after m iterations, we obtain $z'' \equiv z' \pmod{p^m}$, i.e., for $k = 1$ the assertion proved.

Let $z_1 = \Phi_1(z)$, $z_2 = \Phi_2(z)$. Suppose that for $k > 1$ we have

$$\Phi_{k-1}(z_1) \equiv \Phi_{k-2}(z_2) \pmod{p^m} \Leftrightarrow z_1 \equiv z_2 \pmod{p^m}.$$

Consider the congruence

$$\alpha(\Phi_{k-1}(z'))^{-1} + \beta + \gamma k z' \equiv \alpha(\Phi_{k-1}(z''))^{-1} + \beta + \gamma k z'' \pmod{p^m}.$$

If $z' \equiv z'' \pmod{p^{m-\nu_p(\gamma)}}$, then we have

$$\Phi_{k-1}(z') \equiv \Phi_{k-1}(z'') \pmod{p^m} \Rightarrow z' \equiv z'' \pmod{p^m}.$$

Let assume that $z' \not\equiv z'' \pmod{p^{m-\nu_p(\gamma)}}$. But then

$$\begin{aligned}
&\alpha(\Phi_{k-1}(z'))^{-1} + \beta + \gamma k z' \equiv \alpha(\Phi_{k-1}(z''))^{-1} + \beta + \gamma k z'' \pmod{p^{\nu_p(\gamma)}} \Rightarrow \\
&\Rightarrow \alpha(\Phi_{k-1}(z'))^{-1} \equiv \alpha(\Phi_{k-1}(z''))^{-1} \pmod{p^{\nu_p(\gamma)}} \Rightarrow z' \equiv z'' \pmod{p^{\nu_p(\gamma)}} \Rightarrow \\
&\Rightarrow \alpha(\Phi_{k-1}(z'))^{-1} + \beta + \gamma k z' \equiv \alpha(\Phi_{k-1}(z''))^{-1} + \beta + \gamma k z'' \pmod{p^{2\nu_p(\gamma)}} \\
&\Rightarrow z' \equiv z'' \pmod{p^{2\nu_p(\gamma)}}.
\end{aligned}$$

Hence, after $\left[\frac{m}{\nu_p(\gamma)}\right]$ steps we get contradiction with an assumption that $z' \not\equiv z'' \pmod{p^{m-\nu_p(\gamma)}}$, from where it follows the assertion of Lemma 1. □

Henceforth, we will write z_k instead of $\Phi_k(z_0)$, where z_0 is an initial value of recursion (3).

Corollary 1. *The sequence $\{z_n\}$ is a pure periodical with a period $\tau \le p^{2m}\left(1 - \frac{1}{p^\gamma}\right)$.*

Lemma 2. *Let $f(z) = Bz + Cz^2 + p(Dz^3 + \cdots)$ be the polynomial with coefficients over G, and let $(C, p) = 1$. Then for every $A \in G$ we have*

$$\left| \sum_{z \in G^*_{p^m}} e_{p^m}\left(\Re\left(\frac{Az + f(z^{-1})}{p^m}\right)\right)\right| \le 4(N(p^m))^{\frac{1}{2}} = 4p^m. \tag{5}$$

Proof. This assertion is the corollary of the estimate of linear sum

$$\sum_{x \in G_\gamma} e^{\pi i Sp\frac{\alpha x}{\gamma}} = \begin{cases} N(\gamma), & if \quad \alpha \equiv 0 \pmod{\gamma}, \\ 0, & otherwise \end{cases}$$

and of the analogue of estimate of the Gauss sum over finite field. □

Further, we will consider the generator (3) with additional condition $0 < \nu_p(\beta) < \nu_p(\gamma) = r < m$.

Lemma 3. *Let the sequence $\{z_n\}$ is generated by recursion (3), moreover we have $0 < \nu_p(\beta) < \nu_p(\gamma) = r < m$. Then modulo p^m the following relations*

$$\begin{cases} z_{2n} = \dfrac{A_0^{(2n)} + A_1^{(2n)} z_0 + \cdots + A_{r-1}^{(2n)} z_0^{r-1}}{B_0^{(2n)} + B_1^{(2n)} z_0 + B_2^{(2n)} z_0^2 \cdots + B_r^{(2n)} z_0^r} \\ z_{2n+1} = \dfrac{C_0^{(2n+1)} + C_1^{(2n+1)} z_0 + C_2^{(2n+1)} z_0^2 \cdots + C_r^{(2n+1)} z_0^r}{D_0^{(2n+1)} + D_1^{(2n+1)} z_0 + D_2^{(2n+1)} z_0^2 \cdots + D_{r-1}^{(2n+1)} z_0^{r-1}} \end{cases} \tag{6}$$

$$\begin{cases} A_0^{(2n)} = n\alpha^n\beta + \overline{A}_0^{(2n)}\beta^2, \;\; A_1^{(2n)} = \alpha^n + n\overline{A}_1^{(2n)}\beta^2, \\ B_0^{(2n)} = \alpha^n + \overline{B}_0^{(2n)}\beta^2, \;\; B_1^{(2n)} = n\alpha^{n-1}\beta + \overline{B}_1^{(2n)}\beta^3, \\ A_2^{(2n)} \equiv 0 \pmod{p^{2\nu_p(\gamma)}}, \;\; B_2^{(2n)} \equiv n\alpha^{n-1}\gamma \pmod{p^{2\nu_p(\gamma)}}, \\ C_0^{(2n+1)} = \alpha^{n+1}\beta + \overline{C}_0^{(2n+1)}\beta^2, \\ C_1^{(2n+1)} = (n+1)\alpha^n\beta + \overline{C}_1^{(2n+1)}\beta^3, \\ C_2^{(2n+1)} = (n+1)\alpha^n C, \\ D_0^{(2n+1)} = n\alpha^n\beta + \overline{D}_0^{(2n+1)}\beta^3, \\ D_1^{(2n+1)} = \alpha^n + n\alpha^n\gamma + \overline{D}_1^{(2n+1)}\beta^2, \\ D_2^{(2n+1)} \equiv 0 \pmod{p^{2\nu_p(\gamma)}}, \end{cases} \tag{7}$$

$$A_\ell^{(2n)} \equiv B_\ell^{(2n)} \equiv C_\ell^{(2n+1)} \equiv D_\ell^{(2n+1)} \equiv 0 \pmod{p^{\nu_p(\beta)+(\ell-1)\nu_p(\gamma)}}, \; \ell = 3, 4, \ldots.$$

hold,
where $\overline{A}_0^{2n}$, $\overline{B}_0^{2n}$, $\overline{C}_0^{2n+1}$, $\overline{D}_0^{2n+1}$ are polynomials on n with coefficients over G_{p^m}.

Proof. All calculations below will be provided modulo $p^{2\nu_p(c)}$, as it is enough to prove Lemma 4 and all its corollaries. Therefore, in the following we can take that $r = 2$. And then, by induction on n we immediately get an equalities (5).

In order that to prove the relations (6), let consider the following matrices

$$\begin{aligned} A &= \begin{pmatrix} \alpha + \beta^2 & \alpha\beta \\ \beta & \alpha \end{pmatrix}, \;\; A_1 = \begin{pmatrix} \alpha^{-1} + \beta^2 & \beta \\ \alpha^{-1}\beta & 0 \end{pmatrix}, \\ B &= \begin{pmatrix} 2\beta\gamma & 2\gamma \\ \gamma & 0 \end{pmatrix}, \;\; C = \begin{pmatrix} \beta\gamma & 0 \\ \gamma & 0 \end{pmatrix}. \end{aligned} \tag{8}$$

We have,

$$A = \alpha(E + A_1),\ A_1^s \equiv 0 \pmod{p^{s\nu_p(\beta)}},\ s = 1, 2, 3, \ldots, \tag{9}$$

where $E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $O = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

Moreover,

$$A^n \equiv \alpha^n \left(E + nA_1 + \frac{n(n-1)}{2} A_1^2 + \cdots \right) \pmod{p^{2\nu_p(\gamma)}} \tag{10}$$

Calculating z_{n+1}, z_{n+2} from expression for z_n in (5) we get the relations

$$\begin{cases} A_0^{(n+2)} = (\alpha + \beta^2) A_0^{(n)} + \alpha\beta B_0^{(n)}, \\ A_\ell^{(n+2)} = (\alpha + \beta^2) A_\ell^{(n)} + \alpha\beta B_\ell^{(n)} + \\ \qquad + \alpha\gamma(n+2) B_{\ell-1}^{(n)} + \beta\gamma(2n+3) A_{\ell-1}^{(n)}, \end{cases} \tag{11}$$

$$\begin{cases} B_0^{(n+2)} = \alpha B_0^{(n)} + \beta A_0^{(n)}, \\ B_\ell^{(n+2)} = \alpha B_\ell^{(n)} + \beta A_\ell^{(n)} + (n+2)\gamma A_{\ell-1}^{(n)}, \end{cases} \tag{12}$$

where $1 \le \ell \le r$.
Simple calculations give

$$A_0^{(0)} = 0,\ B_0^{(0)} = 1,\ A_1^{(0)} = 1,\ B_1^{(0)} = 0,\ A_2^{(0)} = 0,\ B_2^{(0)} = 0,$$
$$A_0^{(1)} = \alpha,\ B_0^{(1)} = \beta,\ A_1^{(1)} = \beta,\ B_1^{(1)} = 1,\ A_2^{(1)} = \gamma,\ B_2^{(1)} = 0.$$

Let $n = 2n_1 + t$, where

$$t = \begin{cases} 0, & if \quad n \text{ is even}, \\ 1 & if \quad n \text{ is odd}. \end{cases}$$

Now, from (7)-(10) we obtain for even n modulo p^m

$$\begin{pmatrix} A_0^{(n)} \\ B_0^{(n)} \end{pmatrix} \equiv A^{n_1} \begin{pmatrix} A_0^{(0)} \\ B_0^{(0)} \end{pmatrix},$$

$$\begin{pmatrix} A_1^{(n)} \\ B_1^{(n)} \end{pmatrix} \equiv A^{n_1} \begin{pmatrix} A_1^{(0)} \\ B_1^{(0)} \end{pmatrix} + \left[\sum_{j=0}^{n_1-1} (n-2j) A^j B A^{n_1-j-1} - \right.$$

$$\left. - \sum_{j=0}^{n_1-1} A^j C A^{n_1-j-1} \right] \begin{pmatrix} A_o^{(0)} \\ B_0^{(0)} \end{pmatrix} \equiv$$

$$\equiv \left(\alpha^{n_1} \left(E + k_1 A_1 + \frac{k_1(k_1-1)}{2} A_1^2 + \cdots \right) \right) \begin{pmatrix} A_1^{(0)} \\ B_1^{(0)} \end{pmatrix} +$$

$$+ \left[2 \sum_{j=0}^{n_1-1} (n_1-j) \alpha^{n_1-1} \left(E + jA_1 + \frac{j(j-1)}{2} A_1^2 + \cdots \right) BA' - \right.$$

$$- \sum_{j=0}^{n_1-1} \alpha^{n_1-1} \left(E + jA_1 + \frac{j(j-1)}{2} A_1^2 + \cdots \right) CA'' +$$

$$\left. + \alpha^{n_1-1} \beta^2 \gamma n D_1(n) \right] \begin{pmatrix} A_0^{(0)} \\ B_0^{(0)} \end{pmatrix},$$

where

$$A' = \left(E + (n_1 - j - 1) A_1 + \frac{(n_1-j-1)(n_1-j-1)}{2} A_1^2 + \cdots \right).$$

Analogically,

$$\begin{pmatrix} A_2^{(n)} \\ B_2^{(n)} \end{pmatrix} = A^{n_1} \begin{pmatrix} A_2^{(0)} \\ B_2^{(0)} \end{pmatrix} + \left[2\alpha^{n_1-1} \sum_{j=0}^{n_1-1} (n_1-j)(E + jA_1 + \cdots) BA' - \right.$$

$$\left. - \alpha^{n_1-1} \sum_{j=0}^{n_1-1} (E + jA_1 + \cdots) CA' + \alpha^{n_1-1} \beta^3 \gamma n D_2(n) \right] \begin{pmatrix} A_1^{(0)} \\ B_1^{(0)} \end{pmatrix},$$

where $D_1(n)$, $D_2(n)$ are the matrices of order II with coefficients over $G_{p^m}[n]$.

Hence, for $n = 2n_1$ we straight obtain the equalities (5) and (6); and for $n = 2n_1 + 1$ the equalities (5) and (6) be the corollaries of recursion (3) for z_{2n+1}. □

Lemma 4. *Let p be a prime, $p > 3$, $p \equiv 4 \pmod 4$, and let $m \in \mathbb{N}$, $m \geq 3$, $\alpha, \beta, \gamma \in G$, $(\alpha, p) = 1$, $0 < \nu_p(\beta) = \nu < \mu = \nu_p(\gamma)$. Then for Gaussian*

integers z_n generated by recursion (3), we have

$$\begin{aligned} z_{2n} &= (n\beta - 2^{-1}n(n^2-1)\alpha^{-1}\beta^3 + G_0(n)) + \\ &\quad + (1 + (n+1)n\alpha^{-1}\gamma + G_1(n))z_0 + \\ &\quad + (\ -n\alpha^{-1}\beta - (n^3\gamma + n^2(n+1)\alpha^{-1})\beta\gamma + \\ &\qquad + (2^{-1}2n^3 - 2n^2 + 2^{-1}n)\alpha^{-2}\beta^3 + G_2(n))z_0^2 + \\ &\quad + (n^2\alpha^{-2}\beta^2 - n^2\alpha^{-1}\gamma + G_3(n))z_0^3 + G_4(n, z_0)z_0^4; \end{aligned} \tag{13}$$

$$\begin{aligned} z_{2n+1} &= ((n+1)\beta - n^2\alpha^{-1}\gamma + n(n-1)\alpha^{-1}\beta^3 + H_0(n)) + \\ &\quad + ((2n+1)\gamma + H_1(n))z_0 + (\alpha - n^2\gamma - 2n^2\beta^2 + H_{-1}(n))z_0^{-1} + \\ &\quad + (\ -n\alpha\beta + 2^{-1}3n^2(n+1)\beta^3 + \\ &\qquad + 4^{-1}n^2(n^2-1)\alpha^{-1}\beta^3 + H_{-2}(n))z_0^{-2}, \end{aligned} \tag{14}$$

where $G_i(n) \in G[n]$, $G_i(0) = 0$, $G_i(n) \equiv 0 \pmod{p^{\min(2\nu+\mu,4\nu)}}$,
$H_i(n) \in G[n]$, $H_i(0) = 0$, $H_i(n) \equiv 0 \pmod{p^{\min(2\nu+\mu,4\nu)}}$,
$\nu = \nu_p(\beta)$, $\mu = \mu_p(\gamma)$,
moreover, all multiplicative inverses take modulo p^m.

Proof. From (5) it is clear that for every n only one summand in the numerator and denominator is coprime with p. Thus, in formula for z_n, multiplying the numerator and denominator of fraction by multiplicative inverse to denominator, and using p-adic factorization for

$$\frac{1}{1+pu} = 1 - pu + (pu)^2 - \cdots + (-1)^{m-1}(pu)^{m-1} \pmod{p^m}$$

and after simple calculations we obtain the representations for z_{2n} and z_{2n+1} in powers of z_0 and z_0^{-1} modulo p^m. □

Corollary 2. *For* $n = 0, 1, 2, \ldots$ *we have*

$$\begin{aligned} z_{2n} &= \omega_0 + n[b(1 - \alpha^{-1}z_0^2) + 2\alpha^{-1}\beta^3(\alpha + z_0^2) + \alpha^{-1}\gamma z_0 + C_1(z_0)] + \\ &\quad + n^2(\gamma(\alpha^{-1} - z_0^{-1}) + D_2(z_0, z_0^{-1}) + n^3 D_3(n, z_0, z_0^{-1})), \end{aligned}$$

where $C_1(z_0) \equiv C_2(z_0) \equiv C_3(n, z_0) \equiv 0 \pmod{p^{\min(\nu+\mu,3\nu)}}$,
$D_1(z+0, z_0^{-1}) \equiv D_2(z_0, z_0^{-1}) \equiv D_3(n, z_0, z_0^{-1}) \equiv 0 \pmod{p^{\min(\nu+\mu,3\nu)}}$,
for every $z_0, z_0^{-1} \in G_{p^m}^*$, $n \in \mathbb{N}$,
$\nu = \nu_p(\beta)$, $\mu = \nu_p(\gamma)$.

Corollary 3. *Let* τ *be the least period of sequence* $\{z_n\}$ *generated by recursion (3), and* $0 < \nu_p(\beta) < \nu_p(\gamma) < m$. *Then*

(i) $\tau = 2p^{m-\nu}$, *if* $\alpha \not\equiv z_0^2 \pmod p$;

(ii) $\tau = 2p^{m-\nu-\nu_p(\alpha-z_0^2)}$, *if* $0 < \nu_p(\alpha - z_0^2) < \min(3\nu, \mu)$;

(iii) $\tau \le 2p^{m-\nu-\min(2\nu,\mu)}$ *in other cases.*

3. Main Results

For arbitrary Gaussian integers h_1, h_2 let consider the sum

$$\sigma_{k\ell}(h_1, h_2) := \sum_{z_0 \in G^*_{p^m}} e^{\pi i Sp\left(\frac{h_1 z_k + h_2 z_\ell}{p^m}\right)}.$$

Here, we consider z_k, z_ℓ as functions in z_0 with description in Lemma 4.

Theorem 4. *Let* $gcd(h_1, h_2, p^m) = p^s$, $s \le m$, $h_1 = h_1^{(0)} p^s$, $h_2 = h_2^{(0)} p^s$, $gcd(h_1^{(0)}, h_2^{(0)}, p) = 1$, $\nu_p((h_1 + h_2, p^m)) = t \ge s$, $h_1^{(0)} k + h_2^{(0)} \ell, p^{m-s} = p^r$. *The following estimate*

$$|\sigma_{k,\ell}(h_1, h_2)| \le \begin{cases} 0, & if \quad t \ne r+\nu,\ \min(t, r+\nu) < m-s-\nu, \\ 2p^{m+\nu+s+t}, & if \quad t = r+\nu,\ m-\nu-t > 0, \\ \widetilde{\varphi}(p^m), & if \quad \min(t, r+s) \ge m-s-\nu, \end{cases}$$

holds, where $\widetilde{\varphi}(p^m) = p^{2m}\left(1\frac{1}{p^r}\right)$ *be the Euler function over* G; $\nu = \nu_p(\beta)$.

Proof. Let's begin with assumption that k and ℓ are the nonnegative integers with different parity. And let us agree to write z instead z_0. By the Lemma 4 we may write

$$\begin{aligned} h_1 z_{2k} + h_2 z_{2\ell+1} &= p^s \left[(A_0 + A_1 z + A_2 z^2 + A_3 z^3 + \beta^3 z^4 H(z)) + \right. \\ &\left. + (A_{-1} z^{-1} + A_{-2} z^{-2} + A_{-3} z^{-3} + \beta^3 z^{-4} G(z^{-1}))\right] := \\ &:= p^s F(z, z^{-1}), \end{aligned} \tag{15}$$

where

$$\begin{aligned} &A_1 \equiv h_1^{(0)} \pmod{p^\nu},\ A_2 \equiv -k\beta\alpha^{-1} h_1^{(0)} \pmod{p^{\nu+1}}, \\ &A_{-1} \equiv a h_2^{(0)} \pmod{p^\nu},\ A_{-2} \equiv h_2^{(0)} \alpha\ell\beta \pmod{p^{\nu+1}}, \\ &A_3 \equiv A_{-3} \equiv 0 \pmod{p^{\nu+1}}. \end{aligned}$$

Let

$$z = u + p^{m-1-s} v,\ u \in G^*_{p^{m-1-s}},\ v \in G_p. \tag{16}$$

Then, we have

$$z^{-1} \equiv u^{-1} - p^{m-1}u^{-2}v \pmod{p^m},$$
$$z^{j} \equiv u^{j} + jp^{m-1}u^{j-1}v \pmod{p^m},$$
$$z^{-j} \equiv u^{-j} - jp^{m-1}u^{-j-1}v \pmod{p^m}.$$

Hence,

$$p^{-s}(h_1 z_{2k} + h_2 z_{2\ell+1}) \equiv (F(u,u^{-1}) + (h_1^{(0)} - h_2^{(0)}\alpha u^{-2})p^{m-s-1}u) \pmod{p^{m-s}}.$$

Now, by substituting the value of z from (15) and by summing over v, in virtue of classical estimation of the complete linear sum over G_p, we deduce

$$|\sigma_{k,\ell}(h_1,h_2)| = N(p^{s+1}) \left| \sum_{\substack{u \in G^*_{p^{m-s-1}} \\ h_1^{(0)}u^2 \equiv h_2^{(0)}\alpha \pmod{p}}} e^{\pi i Sp\left(\frac{F(u,u^{-1})}{p^{m-s}}\right)} \right| \leq$$
$$\leq 2N(p^{s+1}) \left| \sum_{u,u^{-1} \in G^*_{p^{m-s-2}}} e^{\pi i Sp\left(\frac{F_1(u,u^{-1})}{p^{m-s-2}}\right)} \right|, \tag{17}$$

where $F_1(u,u^{-1})$ be the polynomial with coefficients from $G_{p^{m-s-2}}$ and has the same view as the polynomial $F(u,u^{-1})$. Continuing these discourses, we obtain the assertion of lemma for $k \not\equiv \ell \pmod 2$.

Let k and ℓ be the numbers of same parity (for example, $k = 2k_1$, $\ell = 2\ell_1$). Then modulo p^{m-s}, we have

$$p^{-s}(h_1 z_{2k} + h_2 z_{2\ell}) \equiv B_0 + B_1 z + B_2 z^2 + B_3 z^3 + z^4 B_4(z) : F(z), \tag{18}$$

where

$$B_1 = h_1^{(0)} + h_2^{(0)} + pB_1',$$
$$B_2 = \alpha^{-1}\beta(h_1^{(0)}k + h_2^{(0)}\ell) + p^{2\nu}B_2',$$
$$B_3 = (\alpha^{-2}\beta^2 - \alpha^{-1}\gamma)(h_1^{(0)}k^2 + h_2^{(0)}\ell^2) + p^{3\nu}B_3',$$
$$B_4(z) = p^{2\nu+\mu}B_4'(z),$$

moreover, the coefficients in $B_4'(z) \in G[z]$ contain the multipliers type of $h_1k^j + h_2\ell^j$, $j \geq 0$, and B_1', B_2', B_3' are comprised of multipliers type of $\delta(h_1k^j + h_2\ell^j)$, $\delta \in G$.

By induction on j it is easy to show that

$$h_1^{(0)}k^j + h_2^{(0)}\ell^j \equiv 0 \pmod{p^t},$$

only if

$$h_1^{(0)} + h_2^{(0)} \equiv h_1^{(0)} k + h_1^{(0)} \ell \equiv 0 \pmod{p^t}$$

for some t.
Thus, as above, we conclude

$$p^{-s}(h_1 z_{2k} + h_2 z_{2\ell}) \equiv F(u) + p^{m-s-1} z(B_1 + 2B_2 u) \pmod{p^{m-s}}.$$

By virtue of lemma we infer

$$|\sigma_{k,\ell}(h_1, h_2)| \le \begin{cases} 0, & if \quad t \ne r+\nu,\ \min(t, r+\nu) < m-s-\nu, \\ 2p^{m+\nu+s+t}, & if \quad t = r+\nu,\ m-\nu-s-t > 0, \\ p^{2m}\left(1 - \frac{1}{p^2}\right), & if \quad \min(t, r+v) \ge m-s-\nu. \end{cases}$$

In case $k \equiv \ell \equiv 1 \pmod 2$ the proof is the same. □

Let $h \in G$, $(h, p^m) = p^s$, $0 \le s < n$, and let τ be the least period of sequence $\{z_n\}$, $n = 0, 1, 2, \ldots$ generated by recursion (3).

For $1 \le N \le \tau$ we define the sum

$$S_N(h, z_0) = \sum_{n=0}^{N-1} e^{\pi i Sp\left(\frac{hz_n}{p^m}\right)}. \tag{19}$$

Theorem 5. *Let $\{z_n\}$ be the sequence generated by recursion (3) with a period $\tau = 2p^{m-\nu}$, and let $2\nu < \mu$. Then*

$$|S_\tau(h, z)| \le \begin{cases} 0, & if \quad \nu + s < m, \\ \tau, & if \quad \nu + s \ge m. \end{cases} \tag{20}$$

Proof. As $\tau = 2p^{m-\nu}$ is a maximal possible period for the sequences generated by (3), we may conclude that $gcd(a - z^2, p) = gcd(1 - az^{-2}, p) = 1$. And, therefore, by Corollary 1 of Lemma 2 we obtain

$$\begin{aligned} S_\tau(h, z) &= \sum_{\substack{n_1=0 \\ n=2n_1}}^{p^{m-\nu}-1} e^{\pi i Sp\left(\frac{hz_n}{p^m}\right)} + \sum_{\substack{n_1=0 \\ n=2n_1+1}}^{p^{m-\nu}-1} e^{\pi i Sp\left(\frac{hz_n}{p^m}\right)} = \\ &= \sum_{n=0}^{p^{m-\nu}-1} e^{\pi i Sp\left(\frac{hF(n)}{p^m}\right)} + \sum_{n=0}^{p^{m-\nu}-1} e^{\pi i Sp\left(\frac{hG(n)}{p^m}\right)}, \end{aligned} \tag{21}$$

where the polynomials $F(u)$ and $G(u)$ have the following representation

$$F(u) = f_0 + p^\nu f_1 n + p^{2\nu}(f_2 n^2 + f_3 n^3 + \cdots),$$
$$G(u) = g_0 + p^\nu g_1 n + p^{2\nu}(g_2 n^2 + g_3 n^3 + \cdots),$$

moreover $(f_1, p) = (g_1, p) = 1$.

Therefore, the last two sums on the right in (20) may be simply reduced to complete linear sums, such that

$$S_\tau(h,z) = p^s \left\{ e^{\pi i Sp\left(\frac{f_0 h^{(0)}}{p^{m-s}}\right)} \sum_{n=0}^{p^{m-s-\nu}} e^{\pi i Sp\left(\frac{f_1 n}{p^{m-s-\nu}}\right)} + \right.$$

$$\left. + e^{\pi i Sp\left(\frac{g_0 h^{(0)}}{p^{m-s}}\right)} \sum_{n=0}^{p^{m-s-\nu}} e^{\pi i Sp\left(\frac{g_1 n}{p^{m-s-\nu}}\right)} \right\} =$$

$$= \begin{cases} 0, & if \quad \nu + s < m \\ \delta\tau, & if \quad \nu + s \geq m, \end{cases}$$

where $\delta = e^{\pi i Sp\left(\frac{f_0 h^{(0)}}{p^{m-s}}\right)} + e^{\pi i Sp\left(\frac{g_0 h^{(0)}}{p^{m-s}}\right)}$.

Theorem 2 proved. □

Theorem 6. *Let $\{z_n\}$ be the sequence generated by recursion (3), and let $0 < \nu_p(\alpha - z_0^2) < \min(3\nu, \mu)$, moreover $2\nu < \mu$. Then the sequence $\{z_n\}$ has a period $\tau < 2p^{m-\nu}$, and the following estimates*

$$|S_\tau(h,z)| \leq$$

$$\begin{cases} 0, & if \quad 0 < \nu_p(\alpha - z^2) < \nu \quad and \quad \nu_p(\alpha - z^2) < m - \nu - s; \\ \tau, & if \quad 0 < \nu_p(\alpha - z^2) < \nu \quad and \quad \nu_p(\alpha - z^2) \geq m - \nu - s; \\ 4p^{\frac{m+s+2\nu}{2}}, & if \quad \nu_p(\alpha - z^2) \geq \nu \quad and \quad 2\nu + s \leq m; \\ \tau, & if \quad \nu_p(\alpha - z^2) \geq \nu \quad and \quad 2\nu + s < m \end{cases}$$

hold.

The proof of Theorem 3 is the same to proof of Theorem 2, taking into account the Corollaries 1 and 2 of Lemma 4.

Theorem 7. *Let the sequence $\{z_n\}$ is generated by recursion (3) and has a period τ, moreover $0 \leq \nu_p(\alpha - z^2) < \nu$, $2\nu < \mu$, $\nu_p(h) = s$, $h \in G$. Then, for $0 < N \leq \tau$ the following estimate*

$$|S_N(h,z)| \leq \begin{cases} N, & always, \\ 2p^{\frac{m+s+\nu}{2}} \left(\frac{N}{\tau} + \frac{\log \tau}{p}\right), & if \quad \nu + s < m \end{cases}$$

holds.

This theorem is the corollary of Lemma 2 and estimate of sum through the compete sum.

4. Conclusion

In conclusion, we note that the estimates of exponential sums, obtained in Theorems 1-4, are essencially use the representation of z_n in the form of polynomials in z_0, z_0^{-1} or in n. These representations are also allowed to obtain the nontrivial estimates for exponential sums over s-dimentional points of the form $(z_n, z_{n+1}, \ldots, z_{n+s-1})$, and so it makes possible to investigate such sums on passes the s-dimentional serial tests on statistical independence of the elements of sequence $\{z_n\}$.

References

[1] Chou W.-S. On inversive maximal period polynomials over finite fields. Appl. Algebra Engrg. Comm. Comput..- Vol. 6.- 1995.- P.245-250.

[2] Chou W.-S. The period lengths of inversive congruential recursions. Acta Arith.- 73(4).- 1995.- P.325-341.

[3] Eichenauer J. and Lehn J. A non-linear congruential pseudorandom numbers generator, Statist. Hefte.- 27.- 1986.- P.315-326.

[4] Eichenauer-Herrmann J., Grothe H. A new inversive congruential pseudorandom number generator with power of two modulus ACM Transactions of Modeling and Computer Simulation.- 1992.- 2(1).- P.1-11.

[5] Eichenauer J., Lehn J. and Topuzo lu A. A nonlinear congruential pseudorandom number generator with power of two modulus Math. Comp.- 1988.- 51.- P.757-759.

[6] Eichenauer-Herrmann J., Niederreiter H. Lower bounds for the discrepancy of inversive congruential pseudorandom numbers with power of two modulus Math. Comp..- 1992.- 58.- P.775779.

[7] Eichenauer-Herrmann J., Topuzo lu A. On the period of congruential pseudorandom number sequences generated by inversions J. Comput. Appl. Math..- 1990.- 31.- P.87-96.

[8] Eichenauer-Herrmann J. Construction of inversive congruential pseudoramdom number generators with maximal period length J. Comput. Appl. Math..- 1992.- 40.- P.345-349.

[9] Eichenauer-Herrmann J. Improved lower bounds for the discrepancy of inversive congruential pseudorandom numbers Math. Comp..- 1994.- 62.- P.783-786.

[10] Huber K. On the period length of generalized inversive pseudorandom generators Appl. Algebra Engrg. Comm. Comput..- 1994.- 5.- P.255-260.

[11] Kato T., Wu L.-M., Yanagihara N. On a nonlinear congruential pseudorandom number generator Math. Comput..- 1996.- 65(213).- P.227-233.

[12] Niederreiter H. Random Number Generation and Quasi-Monte Carlo Methods / SIAM, Philadelphia.- 1992.

[13] Niederreiter H., Shparlinski I. On the Distribution of Inversive Congruential Pseudorandom Numbers in Parts of the Period Math. of Comput..- 2000.- 70.- P.1569-1574.

[14] Niederreiter H., Shparlinski I. Exponential sums and the distribution of inversive congruential pseudorandom numbers with prime-power modulus Acta Arith..- 2000.- 90(1).- P.89-98.

[15] Vaaler J. D. Some extremal functions in Fourier analysis Bull. Amer. Math. Soc. (N.S.).- 1985.- 12.- P.183-216.

[16] Varbanets S. On inversive congruential generator for pseudorandom numbers with prime power modulus Annales Univ. Sci. Budapest, Sect. Comp..- 2008.- 29.- P.277-296.

[17] Varbanets P., Varbanets S. Exponential sums on the sequences of inversive congruential pseudorandom numbers with prime-power modulus Vorono's Impact on modern science, Proceedings of the 4th International Conference on Analytic Number Theory and Spatial Tessellations, Book 4, Volume 1, Kyiv, Ukraine.- September 22-28, 2008.- P.112-130.