Annales Univ. Sci. Budapest., Sect. Comp. 44 (2015) 211–219

CONGRUENTIAL GENERATOR OF COMPLEX PSEUDO-RANDOM OF NUMBERS

Tran The Vinh (Odessa, Ukraine)

Communicated by Imre Kátai

(Received August 26, 2015; accepted September 15, 2015)

Abstract. The sequences of complex pseudo-random of numbers (PRN's) producing by powers of generating element of the norm group E_m in the residue class ring modulo p^m (p is a rational prime) over the ring of Gaussian integers are studied.

1. Introduction

We consider the sequence of complex numbers $\{z_n\}$, $|z_n| \le 1$. Let $0 \le \xi_1 < < \xi_2 \le 1$, $0 \le \varphi_1 < \varphi_2 \le 2\pi$, $N(z) = |z|^2$, and let $P(\xi, \varphi)$ denotes the sectorial region of unit circle $|z| \le 1$

(1) $$P = P(\xi, \varphi) := \{z \in \mathbb{C} : \ \xi_1 < N(z) \le \xi_2, \ \varphi_1 < \arg z \le \varphi_2\}.$$

Denote by $\mathfrak{F}$ the collection of sectorial regions $P(\xi, \varphi)$ for all ξ and φ.

We say that the sequence $\{z_n\}$ is pseudo-random in the unit circle if it is induced by a determinative algorithm and its statistic properties are "similar" to the property of the sequence of the random numbers. The "similarity"

Key words and phrases: Gaussian integers, the sequence of pseudo-random numbers, discrepancy.
2010 Mathematics Subject Classification: 11K45, 11T71, 94A60, 11L07, 11T23.
This work was completed with the support of the Hungarian and Vietnamese TET (grant agreement no. TET 10-1-2011-0645).

means that this sequence closely adjacent to uniformly distributed in the disk $|z| \leq 1$, and its elements are uncorrelated. On these properties of the sequence of pseudo-random numbers (abbreviation: PRN's) can destine by value of discrepancy D_N of the points $z_1, z_2, \ldots, z_N$:

$$D_N(z_1, \ldots, z_N) := \sup_{P \subset \mathbb{C}_1} \left| \frac{A_N(P)}{N} - \frac{|P|}{\pi} \right|, \tag{2}$$

where $\mathbb{C}_1 := \{z \in \mathbb{C},\ |z| \leq 1\}$; $A_N(P)$ is the number of points among $z_1, \ldots, z_N$ falling into P, $|P|$ denotes the volume P; supremum is extended over all sectorial region P of unit circle $|z| \leq 1$.

The similar definition of discrepancy D_N has for the s-dimensional sequence of complex points $Z_n^{(s)} = \left(z_1^{(s)}, \ldots, z_n^{(s)}\right)$, $z_j \in \mathbb{C}$.

We say that the sequence z_n passes the s-dimensional test on uncorrelatedness if it passes the s-dimensional test on equidistribution
(i.e. $D_N^{(s)}\left(z_1^{(s)}, \ldots, z_N^{(s)}\right) \to 0$ at $N \to \infty$).

For the construction of the sequence of PRN's on $[0, 1)$ frequently the congruential recursion of the form

$$y_{n+1} \equiv f(y_n) \pmod{m},$$

is used, where $f(u)$ is an integral-valued function.

We will investigate the sequence of complex numbers produced by recursion

$$z_{n+1} \equiv z_0 \cdot (u + iv)^n \pmod{p^m} \tag{3}$$

where z_0 and $u+iv$ are Gaussian integers, $(z_0, p) = 1$; $u^2+v^2 \equiv \pm 1 \pmod{p^m}$.

For real sequences x_n produced by congruential recursion, an estimate for D_N can be obtained by the Erdős–Turán–Koksma inequality (see,[3, Th. 3.10].

In our paper we get an analogue of the Erdős–Turán–Koksma inequality for the sequence of pseudorandom complex numbers. And then we show that the sequence generated by (3) is a sequence of PRN's in $\mathbb{C}_1$.

2. Preliminary results

Notation. Let G denote the ring of the Gaussian integers, $G := \{a+bi :\ a, b \in \in \mathbb{Z}\}$; $N(z) = |z|^2$ be the norm of $z \in G$. For $\gamma \in G$ denote G_γ (respectively, G_γ^*) the complete system of residues (respectively, reduced residues system) in G modulo γ; p is a prime number in $\mathbb{Z}$; $\mathfrak{p}$ is a Gaussian prime number. If q is a positive integer, $q > 1$, then we write $e_q(x) = e^{2\pi i \frac{x}{q}}$ for $x \in \mathbb{R}$. Symbols "O" and "$\ll$" are equivalent; $\nu_p(\alpha) = k$ if $\mathfrak{p}^k|\alpha$, $\mathfrak{p}^{k+1} \nmid \alpha$.

Let $M > 1$ be a positive integer and let $y_1, y_2, \ldots, y_N$ be some sequence of points from G_M and let $Y_M = \{\frac{y_n}{M} | n = 0, \ldots, N-1\}$. For $P \in \mathfrak{F}$ denote $A(P, Y_M)$ the number of points from Y_M contained in P.

We will adapt the proof from [2] for an analogue of the Erdős–Turán–Koksma inequality.

We define the adequate approximation of sectorial region $P \in \mathfrak{F}$,

$$P := \left\{ \frac{z}{q} :\ z \in G,\ N_1 \le N(z) \le N_2,\ 0 \le \varphi_1 < \arg z \le \varphi_2 < 2\pi \right\},\ q \in \mathbb{N}.$$

We say that the set $S(P)$ is the adequate approximation of P if

- (i) $A(P, Y_N(M)) = A(S(P), Y_N(M)) + O\left(N^{\frac{1}{2}}\right)$,
- (ii) volumes $|P|$ and $|S(P)|$ are "similar",
- (iii) $A(S(P), Y_N(M))$ has a representation by an exponential sum.

Let N_1, N_2, φ_1, φ_2 be the parameters in the definition of P. For $r, s \in \mathbb{Z}_M$ we set $\overline{r} = \frac{r}{M}$, $\overline{s} = \frac{s}{M}$.

Determine

(4)
$$S_{\overline{r},\overline{s}} : \left\{ \beta = \frac{\alpha}{M} :\ \alpha \in G_M,\ \overline{r} < N(\beta) \le \overline{r} + \frac{1}{M},\ 2\pi\overline{s} < \arg\alpha \le 2\pi\left(\overline{s} + \frac{1}{M}\right) \right\}.$$

Put

$$S(P) := \bigcup_{\substack{\overline{r},\overline{s} \\ S_{\overline{r},\overline{s}} \subset P}} S_{\overline{r},\overline{s}}.$$

It is obvious that $S(P) = P(\overline{N}_1, \overline{N}_2, \psi_1, \psi_2)$, where

$$\overline{N}_1 = \min\left\{ \frac{a}{M},\ a \in \mathbb{Z}_M :\ N_1 \le \frac{a}{M} \right\}$$

$$\overline{N}_2 = \min\left\{ \frac{b}{M},\ b \in \mathbb{Z}_M :\ N_2 \le \frac{b}{M} \right\}$$

$$\psi_1 = \min\left\{ \frac{2\pi a}{M},\ a \in \mathbb{Z}_M :\ \psi_1 \le \frac{2\pi a}{M} \right\}$$

$$\psi_2 = \min\left\{ \frac{2\pi b}{M},\ b \in \mathbb{Z}_M :\ \psi_2 \le \frac{2\pi b}{M} \right\}.$$

We proved the following analogue of the Erdős–Turán–Koksma inequality (see, [3])

Theorem 1. *Let $M > 1$ be integer. Then for any sequence $\{y_n\}$, $y_n \in G_M$, the discrepancy D_N of points $\left\{\frac{y_n}{M}\right\}$ satisfies the inequality*

$$D_N \leq 2\left(1-\left(1-\frac{2\pi}{M}\right)^2\right)+$$
$$+\frac{1}{M}\sum_{\substack{\gamma\in G_M\\ \gamma\neq 0}}\min\left(\frac{1}{|\sin\pi\Re(\gamma)|},\frac{1}{|\sin\pi\Im(\gamma)|}\right)\frac{1}{N}\left(|S_N|+O\left(N^{\frac{1}{2}}\right)\right),$$

where $S_N = \sum\limits_{n=0}^{N-1} e_M(\Re(\gamma y_n))$.

Proof. By an analogue with the work [2] we infer

$$R_N(S(P)) := \frac{A(S(P))}{N} - |S(P)| = \frac{1}{N}\sum_{n=0}^{N-1}\chi_{S(P)}(x_n) - |S(P)|, \tag{5}$$

where $x_n = \frac{y_n}{M}$, χ_Δ is the characteristic function of the set Δ.

By the equality

$$\chi_{S_{\overline{r},\overline{s}}}(x) = \sum_{\alpha\in S_{\overline{r},\overline{s}}}\frac{1}{M^2}\sum_{\gamma\in G_M} e_M(\gamma(\alpha - x))$$

we get

$$|R_N(S(P))| \leq$$
$$\leq \sum_{0\neq\gamma\in G_M}\tfrac{1}{M^2}\left|\sum_{z(r,s)\in S_{\overline{r},\overline{s}}} e_M(-\Re(\gamma z(r,s)))\right|\cdot\left|\tfrac{1}{N}\sum_{n=0}^{N-1} e_M(\Re(\gamma y_n))\right|, \tag{6}$$

where $z(r,s)$ is the complex number such that

$$N(z(r,s)) = \frac{r}{M},\ \arg z(r,s) = \frac{2\pi s}{M}.$$

In order to calculate the first inner sum over $S_{\overline{r},\overline{s}}$ one needs an estimate of the sum

$$\sum\nolimits_M = \sum_{\substack{N_1<N(\omega)<N_2\\ \varphi_1\leq\arg\omega\leq\varphi_2}} e_M(\Re(\gamma\omega)),\ (0\neq\gamma\in G_M). \tag{7}$$

The sum $\sum_M$ can be considered as a sum of coefficients of the next Dirichlet series for the Hecke Z-function over the Gaussian field $\mathbb{Q}(i)$:

$$Z_m(s,\delta_0,\delta_1)=\sum_{0\neq\omega\in G}\frac{e^{2\pi i\Re(\omega\delta_1)}}{N(\omega+\delta_0)^s}e^{4mi\arg\omega},\ (\Re s>1).$$

Putting $\delta_0=0$, $\delta_1=\frac{\gamma}{M}$, we obtain for any $T>1$ by a standard way the following estimates:

$$\sum_{N(\omega)\le X}e_M(\gamma\omega)=(\varphi_2-\varphi_1)\sum N(\omega)\le xe_M(\gamma\omega)+O\left(\frac{1}{T}\sum_{N(\omega)\le x}1\right)+ \tag{8}$$
$$+O\left((\varphi_2-\varphi_1)\sum_{m=1}^{T}\left|\sum_{N(\omega)\le x}e_M(\gamma\omega)e^{4mi\arg\omega}\right|\right).$$

$$\sum_{N(\omega)\le x}e_M(\gamma\omega)e^{4mi\arg\omega}\ll_\varepsilon\frac{x^{\frac12+\varepsilon}}{M^{\frac14}}+M^{\frac12}(|m|+3)^{1+\varepsilon} \tag{9}$$

(for the details, see Chapter 2 of [1], for example).

Next, we have a simple analogue of the estimate of linear exponential sum over G

$$\left|\sum_{N_1<N(\omega)\le N_2}2^{2\pi i\Re(\alpha\omega)}\right|\le \tag{10}$$
$$\le(N_2-N_1)^{\frac12}\min\left((N_2-N_1)^{\frac12},\frac{1}{|\sin\pi\Re(\alpha)|},\frac{1}{|\sin\pi\Im(\alpha)|}\right).$$

Now by (4)–(9), putting $T=x^{\frac23}$ and taking into account that $|P|=$ $=\frac{\varphi_2-\varphi_1}{2}(N_2-N_1)$, we obtain our assertion. ■

3. Sequence of PRNs produced by the cyclic group E_n

Let $p\equiv 3\pmod 4$ be a prime integer. Consider the set of the classes of residue $\pmod{p^n}$ over G, such that for every $\alpha\in E_n$ we have $N(\alpha)\equiv\pm1\pmod{p^n}$. Respectively for a convolution of multiplication the set E_n forms a group. It is well known that a regular generative element of E_1 (i.e. $u^2+v^2\equiv-1\pmod p$), $u^2+v^2=-1+ph$, $(h,p)=1$) is a generative element for any E_ℓ,

$\ell = 1, 2, \ldots, n$. Moreover, $|E_n| = 2(p+1)p^{n-1}$ ($|E_n|$ is the number of elements in E_n).

We fix the generative element of E_n and let some $z_0 \in G_n$, $(N(z_0), p) = 1$. We call z_0 an initial value for the sequence $\{z_m\}$, where $z_m = z_0(u+iv)^m$, $m = 0, 1, \ldots, N-1$.

Lemma 1 (([4], pp. 232–233)). *Let $p \equiv 3 \pmod 4$, $n > 3$, and let $u + iv$ is a generative element of the group E_n. Then for every $0 \le \ell \le p^{n-2}$, $0 \le k < < 2(p+1)$, we have*

$$(u+iv)^{2(p+1)p^\ell + k} \equiv A(\ell, k) + iB(\ell, k) \pmod{p^n},$$

where

$$A(\ell, k) \equiv A_0(k) + A_1(k)\ell + \cdots + A_{n-1}(k)\ell^{n-1} \pmod{p^n},$$
$$B(\ell, k) \equiv B_0(k) + B_1(k)\ell + \cdots + B_{n-1}(k)\ell^{n-1} \pmod{p^n},$$

Moreover,

$$A_j(k) = A_j u(k) - B_j v(k),\ B_j(k) = A_j v(k) + B_j u(k),\ j = 0, 1, \ldots, n-1;$$
$$A_0 \equiv 1 \pmod p,\ B_0 \equiv 0 \pmod p;$$
$$A_1 \equiv 0 \pmod{p^3},\ A_2 = p^2 A_2',\ (A_2', p) = 1;$$
$$B_1 = pB_1',\ (B_1', p) = 1,\ B_2 \equiv A_3 \equiv B_3 \equiv \cdots \equiv A_{n-1} \equiv B_{n-1} \equiv 0 \pmod{p^3};$$
$$u(0) = 1,\ v(0) = 0,\ (u(p+1), p) = 1,\ p||v(p+1);$$
$$(v(k), p) = 1 \ for\ k \ne \overline{0, p+1}.$$

Corollary 1.

$$p||A_1(k),\ A_j(k) \equiv 0 \pmod{p^2},\ j = 2, 3, \ldots;\ k \ne \overline{0, p+1};$$
$$p^2||A_1(0),\ A_j(0) \equiv 0 \pmod{p^3},\ j = 2, 3, \ldots;$$
$$p^2||A_1(p+1),\ p^2||A_2(k),\ A_j(p+1) \equiv 0 \pmod{p^3},\ j = 3, 4, \ldots;$$
$$p^2||B_2(k)\ if\ k \ne \overline{0, p+1};\ B_2(k) \equiv 0 \pmod{p^3}\ else;$$
$$B_j(k) \equiv 0 \pmod{p^3},\ j = 3, 4, \ldots; \nu_p(B_1(k)) = 1,\ k = 0, 1, \ldots, 2p+1.$$

Lemma 2. *Let $\alpha \in G_{p^n}$, $\alpha = p^h \alpha_0$, $(\alpha_0, p) = 1$, $h < n$, and let $z_m = z_0(uiv)^m \pmod{p^n}$, $m = 0, 1, \ldots, 2(p+1)p^{n-1} - 1$.*

Then

$$\left| \sum_{j=0}^{N-1} e_{p^{n-1}}(\Re(\alpha z_j)) \right| \le 2p^{\frac{n-h-r-1}{2}},$$

where r is determined from (13)(see, below) and depends on α.

Proof. Let us denote

$$\nu_p(\alpha) = h,\ 0 \le h < n-1,\ \alpha = p^h\alpha_0,\ (\alpha_0, p) = 1;$$
$$M_h = 2(p+1)p^{n-1-h}.$$

Then we have

$$\left|\sum_{m=0}^{M_0-1} e_{p^{n-h-1}}(\Re(\alpha_0 z^m))\right| = p^{2h}\left|\sum_{m=0}^{M_h-1} e_{p^{n-h-1}}(\Re(\alpha_0 z^m))\right| =$$
$$= p^{2h}\left|\sum_{k=0}^{2p+1}\sum_{\ell=0}^{p^{n-h-1}-1} e_{p^{n-h-1}}(aA_k(\ell) - bB_k(\ell))\right|. \tag{11}$$

For every $k = 0, 1, \ldots, 2p+1$, we consider the polynomial

$$aA_k(\ell) - bB_k(\ell) = \sum_{j=0}^{n-1} c_j(k)\ell^j,$$

where

$$c_j(k) = (aA_j - bB_j)u(k) + (bA_j - aB_j)v(k),\ j = 0, 1, \ldots, n-1.$$

In particular,

$$\begin{aligned} c_1(k) &= (aA_1 - bB_1)u(k) + (bA_1 - aB_1)v(k) = \\ &= (au(k) + bv(k))A_1 - (bu(k) - av(k))B_1, \\ c_2(k) &= (aA_2 - bB_2)u(k) + (bA_2 - aB_2)v(k) = \\ &= (au(k) + bv(k))A_2 - (bu(k) - av(k))B_2. \end{aligned} \tag{12}$$

We see that for all values of $k = 0, 1, \ldots, 2p+1$

$$\nu_p(A_1(k)) \ne \nu_p(B_1(k)),\ \nu_p(A_2(k)) \ne \nu_p(B_2(k)).$$

Now if for given α_0 and k the inequality

$$\nu_p(c_1(k)) \ge \nu_p(c_2(k)) = r \tag{13}$$

holds, then the inner sum over ℓ in (11) can be estimated as $p^{\frac{n-h+r-1}{2}}$ (such sum by consequent slope leads to the Gaussian sum).

In other cases (i.e., $\nu_p(c_1(k)) < \nu_p(c_2(k))$) this sum is vanishes.

Hence, from (10)-(12) we infer the assertion of lemma. ■

Lastly we prove the main result

Theorem 2. *Let the sequence $\{z_n\}$ be generated by the recursion*

$$z_{m+1} \equiv z_m(u+iv) \pmod{p^n},$$

where $z_0 \in G_{p^m}$, $u+iv$ is a generative element of the group E_n of classes of residue modulo p^n with the norms that $\equiv \pm 1 \pmod{p^n}$. Then the discrepancy of the points $\left\{\frac{z_m}{p^n}\right\}$, $m = 0,1,\ldots,N-1$, $N \le 2(p+1)p^{n-1}$ satisfies the inequality

$$D_N \le 2\left(1-\left(1-\frac{2\pi}{p^n}\right)^2\right) + N^{-1}p^{\frac{n}{2}}\log p^n.$$

Proof. Indeed, for every h, $0 \le h \le n-1$ there is at most $O(p^{n-h-r})$ numbers α_0, $\alpha_0 \in G_{p^{n-h}}$ for which $\nu_p(c_1(k)) \ge \nu_p(c_2(k)) = r$, where $c_1(k)$, $c_2(k)$ are determined by (11).

Now, by Lemma 2 and Theorem 1 we immediately obtain the theorem. ■

If $A, B \in \mathbb{Z}$, $(B,p) = 1$, then for $A \cdot B^{-1} \pmod{p^n}$ we shall write $\left[\frac{A}{B}\right]_{p^n}$

Remark 1. The characterization of elements for the sequence $\{z_m\}$ (producing by (3)) permits to construct the new sequences of PRN's in interval $[0,1]$ $\Bigg($for example, $\left\{\frac{1}{p^n}\Re(z_m)\right\}$, $\left\{\frac{1}{p^n}\Im(z_m)\right\}$, $\left\{\frac{1}{p^n}\left[\frac{\Re(z_m)}{\Im z_m}\right]_{p^n}\right\}\Bigg)$.

Remark 2. It is possible to deduce from Theorem 1 that the sequence of complex numbers z_n produced by the recursion

$$z_{m+1} \equiv \alpha z_m^{-1} + \beta + \gamma z_m \pmod{p^n},$$

$\alpha,\beta,\gamma,z_0 \in G$, $(\alpha,p) = (z_0,p) = 1$, $\beta \equiv \gamma \equiv 0 \pmod{p}$, passes the s-dimensional test for the equidistribution and unpredictability.

References

[1] **Baker R. C.,** *Diophantine Inequalities*, LMS Monographs (New Series), v.1(Clarendon Press, Oxford), 1986.

[2] **Hellekalen P.,** General discrepancy estimates: the Walsh function system, *Acta Arith.*, **67** (1994), 209–218.

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

[4] **Varbanets S.,** The norm Kloosterman sums over $\mathbb{Z}[i]$, in: *Analytic and Probabilistic Methods in Number Theory*, Proc. Forth. International Conference in Honour of J. Kubilius, Palanga, Lithuania, 25–29 Semtember, 213-224, 2006.

Tran The Vinh
Department of Computer Algebra and Discrete Mathematics
I.I. Mechnikov Odessa National University
65026 Odessa, Dvoryanskaya street 2
Ukraine
ttvinhcntt@yahoo.com.vn