Вісник Одеськ. нац. ун-ту. Матем. і мех. – 2010. – Т.15, вип. 18. – С. 46–58

УДК 511.32

С. А. Задорожный
Одесский национальный университет имени И. И. Мечникова

ИНВЕРСНЫЙ КОНГРУЕНТАЛЬНЫЙ ГЕНЕРАТОР НАД $\mathbb{Z}[i]$

Задорожний С. О. Інверсний конгруентальний генератор над Z[i]. У статті отримана оцінка дискрепанції послідовності псевдовипадкових чисел, генерованих інверсним конгруентним методом над кільцем класів гаусових вичетів по модулю $\mathfrak{p}^m$.
Ключові слова: дискрепанція, інверсний конгруэнтальний метод, числа Гаусса, тригонометрична сума.

Задорожный С. А. Инверсный конгруентальный генератор над Z[i]. В статье получена оценка дискрепанции последовательности псевдослучайных чисел генерируемых инверсным конгруентным методом над кольцом классов гауссовых вычетов по модулю $\mathfrak{p}^m$.
Ключевые слова: дискрепанция, инверсный конгруэнтальный метод, числа Гаусса, тригонометрическая сумма.

Zadorozhny S. A. Inversive congruential generator over Z[i]. The upper bound on the discrepancy of a sequence of pseudorandom numbers generated with inversive congruential method over the ring of residue Gaussian classes modulo $\mathfrak{p}^m$ is presented in the paper.
Key words: discrepancy, inversive congruential method, gaussian numbers, exponential sum.

Введение. Обозначим через $\mathbb{Z}[i]$ кольцо целых гауссовых чисел $\mathbb{Z}[i] = \{a+bi \mid a, b \in \mathbb{Z},\ i^2 = -1\}$. Пусть $\mathfrak{p}$ — простое гауссово число. Через $\mathbb{Z}_{\mathfrak{p}^m}[i]$ будем обозначать полную систему гауссовых вычетов по модулю $\mathfrak{p}^m$, $m \in \mathbb{N}$, $m \geq 2$, а через $\mathbb{Z}^*_{\mathfrak{p}^m}[i]$ приведенную систему гауссовых вычетов.

Выберем $\alpha \in \mathbb{Z}^*_{\mathfrak{p}^m}[i]$, $\beta \in \mathbb{Z}_{\mathfrak{p}^m}[i]$ такое, что $\beta = 0 \pmod{\mathfrak{p}}$. Рассмотрим отображение

$$\psi(w) = \alpha w^{-1} + \beta \pmod{\mathfrak{p}^m}, \tag{1}$$

где $w \in \mathbb{Z}^*_{\mathfrak{p}^m}[i]$, w^{-1} обозначает мультипликативнообратное к w по модулю $\mathfrak{p}^m$. Можно легко проверить, что при выбранных α и β ψ является перестановкой $\mathbb{Z}^*_{\mathfrak{p}^m}[i]$.

Начнем с $w_0 \in \mathbb{Z}^*_{\mathfrak{p}^m}[i]$, затем с помощью рекуррентного соотношения

$$w_{n+1} = \psi(w_n) \qquad n = 0, 1, 2, \ldots$$

сгенерируем последовательность элементов $w_0, w_1, \ldots$ из $\mathbb{Z}^*_{\mathfrak{p}^m}[i]$.

Для любого $\gamma \in \mathbb{C}$ обозначим $Sp(\gamma) = \gamma + \overline{\gamma}$, $N(\gamma) = \gamma \cdot \overline{\gamma}$. Здесь $\overline{\gamma}$ есть комплексно сопряженное к γ. Для любого $r \in \mathbb{R}$ через $\{r\}$ будем обозначать дробную часть числа r.

Рассмотрим последовательность псевдослучайных чисел:

$$\left\{Sp\left(\frac{w_0}{\mathfrak{p}^m}\right)\right\}, \quad \left\{Sp\left(\frac{w_1}{\mathfrak{p}^m}\right)\right\}, \quad \left\{Sp\left(\frac{w_2}{\mathfrak{p}^m}\right)\right\}, \quad \ldots \tag{2}$$

Определим дискрепанцию этих чисел D_M как

$$D_M = \sup_{J\subseteq[0,1)} \left| \frac{A(J,M)}{M} - |J| \right|, \tag{3}$$

где супремум берется по всем подинтервалам J полуинтервала $[0,1)$, $A(J,M)$ — количество точек $\{Sp\,(w_n/\mathfrak{p}^m)\}$, $0 \le n \le M-1$, попавших в интервал J, $|J|$ — длина интервала J.

Инверсный конгруэнтальный генератор над $\mathbb{Z}$ сейчас широко используется как альтернатива линейному конгруэнтальному генератору. Его исследованию посвящено множество работ (см. например [5]–[11]). Инверсный генератор с использованием гауссовых чисел также не лишен интереса. В данной работе мы оцениваем дискрепанцию последовательности (2) на части периода. Для случая поля $\mathbb{Z}_p$ (p — целое простое число) дискрепанция последовательности (2) на части периода была исследована Нидерайтером и Шпарлинским в работе [1], а для кольца $\mathbb{Z}_{p^m}$, $m \ge 2$ в [2]. Мы используем метод, изложенный в этих работах, и обобщаем результат до случая $\mathbb{Z}_{\mathfrak{p}^m}[i]$.

Основные результаты.

1. Вспомогательные результаты.

Если ψ — перестановка заданная (1), r — произвольное целое число, то через ψ^r будем обозначать r-ю степень ψ в группе перестановок группы $\mathbb{Z}^*_{\mathfrak{p}^m}[i]$. Для удобства под записью u/v будем понимать uv^{-1} в мультипликативной абелевой группе. Получим представление $\psi^r(w)$ в виде специальных многочленов. Подобная идея была впервые использована С. Варбанцом при исследовании обобщений инверсного конгруэнтального генератора, см., например, [3].

Теорема 1. *$\psi^r(w)$ можно представить в виде*

$$\psi^r(w) = F^r_+(w) + B^r + F^r_-(w),$$

где при r нечетном:

$$\begin{aligned}
B^r &= \frac{r+1}{2}\beta \pmod{\beta^2} \\
F^r_+(w) &= c^r_1 w + \ldots + c^r_{m-2} w^{m-2} \\
c^r_k &= 0 \pmod{\beta^{k+1}}, \quad k = 1, \ldots, m-2 \\
F^r_-(w) &= c^r_{-1} w^{-1} + \ldots + c^r_{-m} w^{-m} \\
c^r_{-1} &= \alpha \pmod{\beta^2} \\
c^r_{-k} &= 0 \pmod{\beta^{k-1}}, \quad k = 2, \ldots, m,
\end{aligned}$$

при r четном:

$$\begin{aligned} B^r &= 0 \pmod{\beta} \\ F^r_+(w) &= c^r_1 w + \ldots + c^r_m w^m \\ c^r_1 &= 1 \pmod{\beta^2} \\ c^r_2 &= -\frac{r}{2}\alpha^{-1}\beta \pmod{\beta^2} \\ c^r_k &= 0 \pmod{\beta^{k-1}}, \quad k = 3, \ldots, m \\ F^r_-(w) &= c^r_{-1} w^{-1} + \ldots + c^r_{-(m-2)} w^{-(m-2)} \\ c^r_{-k} &= 0 \pmod{\beta^{k+1}}, \quad k = 1, \ldots, m-2 \end{aligned}$$

Доказательство. Доказательство проведем индукцией по r. Проверим базу индукции.

$r = 1$

$$\psi^1(w) = \alpha w^{-1} + \beta.$$

В этом случае имеем $c^1_{-1} = \alpha \pmod{\beta^2}$, $B^1 = \beta \pmod{\beta^2}$

$r = 2$

$$\psi^{-1}(w) = \frac{1}{\alpha w^{-1} + \beta} = \alpha^{-1} w \frac{1}{1 + \alpha^{-1}\beta w}.$$

Воспользуемся разложением в ряд Тейлора и тем, что $\beta = 0 \pmod{\mathfrak{p}}$.

$$\psi^{-1}(w) = \alpha^{-1} w (1 - \alpha^{-1}\beta w + \alpha^{-2}\beta^2 w^2 - \ldots + (-1)^{m-1}\alpha^{-(m-1)}\beta^{m-1} w^{m-1})$$

$$\psi^2(w) = \alpha\psi(w)^{-1} + \beta = w - \alpha^{-1}\beta w^2 + \alpha^{-2}\beta^2 w^3 - \ldots + (-1)^{m-1}\alpha^{-(m-1)}\beta^{m-1} w^m + \beta$$

Имеем $c^2_1 = 1 \pmod{\beta^2}$, $c^2_2 = -\alpha^{-1}\beta \pmod{\beta^2}$. Остальные коэффициенты также удовлетворяют условию теоремы.

Проведем шаг индукции. Для определенности будем считать r четным. Пусть ψ^r представимо в указанном в утверждении теоремы виде и коэффициенты многочленов удовлетворяют соотношениям:

$$\begin{aligned} c^r_1 &= 1 \pmod{\beta^2}, \qquad c^r_2 = -\frac{r}{2}\alpha^{-1}\beta \pmod{\beta^2} \\ c^r_k &= 0 \pmod{\beta^{k-1}}, \quad k = 3, \ldots, m \\ c^r_{-k} &= 0 \pmod{\beta^{k+1}}, \quad k = 1, \ldots, m-2 \\ B^r &= 0 \pmod{\beta}. \end{aligned}$$

Докажем утверждение теоремы для r+1, r+2.

$$\begin{aligned} \psi^{-r}(w) &= w^{-1}(1 + (c^r_1 - 1) + c^r_2 w + c^r_3 w^2 + \ldots + c^r_m w^{m-1} + \\ &\quad + B^r w^{-1} + c^r_{-1} w^{-2} + c^r_{-2} w^{-3} + \ldots + c^r_{-(m-2)} w^{-(m-1)})^{-1} = \\ &= w^{-1} - w^{-1}((c^r_1 - 1) + c^r_2 w + c^r_3 w^2 + \ldots + c^r_m w^{m-1} + \\ &\quad + B^r w^{-1} + c^r_{-1} w^{-2} + c^r_{-2} w^{-3} + \ldots + c^r_{-(m-2)} w^{-(m-1)}) + \\ &\quad + w^{-1}((c^r_1 - 1) + c^r_2 w + c^r_3 w^2 + \ldots + c^r_m w^{m-1} \\ &\quad + B^r w^{-1} + c^r_{-1} w^{-2} + c^r_{-2} w^{-3} + \ldots + c^r_{-(m-2)} w^{-(m-1)})^2 + \ldots + \\ &\quad + (-1)^{m-1} w^{-1}((c^r_1 - 1) + c^r_2 w + c^r_3 w^2 + \ldots + c^r_m w^{m-1} + \\ &\quad + B^r w^{-1} + c^r_{-1} w^{-2} + c^r_{-2} w^{-3} + \ldots + c^r_{-(m-2)} w^{-(m-1)})^{m-1}. \end{aligned} \tag{4}$$

$$\psi^{r+1}(w) = \alpha\psi^{-r}(w) + \beta$$

В скобках вида $w^{-1}(\dots)^t$ из разложения (4) коэффициент при w^{-k}, k — положительное, кратен β^k. Коэффициент при w^k также кратен β^k. Свободный член в скобке $w^{-1}(\dots)^t$ кратен β. Из этого легко вытекает

$$\begin{aligned} c_k^{r+1} &= 0 \pmod{\beta^{k+1}}, \quad k = 1, \dots, m-2 \\ c_{-k}^{r+1} &= 0 \pmod{\beta^{k-1}}, \quad k = 2, \dots, m. \end{aligned}$$

Подсчитаем c_{-1}^{r+1} и B^{r+1} по модулю β^2. Заметим, что скобки $w^{-1}(\dots)^t$, где $t \geq 2$, кратны β^2 и их можно не рассматривать.

$$c_{-1}^{r+1} = \alpha(1 - (c_1^r - 1)) = \alpha \pmod{\beta^2}$$

$$B^{r+1} = \alpha(-c_2^r) + \beta = \frac{r}{2}\beta + \beta = \frac{r+2}{2}\beta \pmod{\beta^2}$$

Рассмотрим $\psi^{r+2}(w)$.

$$\begin{aligned} \psi^{-(r+1)}(w) = {} & \alpha^{-1}w(1 + \alpha^{-1}(c_{-1}^{r+1} - \alpha) + \alpha^{-1}c_{-2}^{r+1}w^{-1} + \dots + \alpha^{-1}c_{-m}^{r+1}w^{-(m-1)} + \\ & + \alpha^{-1}B^{r+1}w + \alpha^{-1}c_1^{r+1}w^2 + \alpha^{-1}c_2^{r+1}w^3 + \dots + \alpha^{-1}c_{m-2}^{r+1}w^{m-1})^{-1} = \\ = {} & \alpha^{-1}w - \alpha^{-1}w(\alpha^{-1}(c_{-1}^{r+1} - \alpha) + \alpha^{-1}c_{-2}^{r+1}w^{-1} + \dots + \alpha^{-1}c_{-m}^{r+1}w^{-(m-1)} + \\ & + \alpha^{-1}B^{r+1}w + \alpha^{-1}c_1^{r+1}w^2 + \alpha^{-1}c_2^{r+1}w^3 + \dots + \alpha^{-1}c_{m-2}^{r+1}w^{m-1}) + \\ & + \alpha^{-1}w(\alpha^{-1}(c_{-1}^{r+1} - \alpha) + \alpha^{-1}c_{-2}^{r+1}w^{-1} + \dots + \alpha^{-1}c_{-m}^{r+1}w^{-(m-1)} + \\ & + \alpha^{-1}B^{r+1}w + \alpha^{-1}c_1^{r+1}w^2 + \alpha^{-1}c_2^{r+1}w^3 + \dots + \alpha^{-1}c_{m-2}^{r+1}w^{m-1})^2 + \dots + \\ & + (-1)^{m-1}\alpha^{-1}w(\alpha^{-1}(c_{-1}^{r+1} - \alpha) + \alpha^{-1}c_{-2}^{r+1}w^{-1} + \dots + \alpha^{-1}c_{-m}^{r+1}w^{-(m-1)} + \\ & + \alpha^{-1}B^{r+1}w + \alpha^{-1}c_1^{r+1}w^2 + \alpha^{-1}c_2^{r+1}w^3 + \dots + \alpha^{-1}c_{m-2}^{r+1}w^{m-1})^{m-1}. \end{aligned} \tag{5}$$

$$\psi^{r+2}(w) = \alpha\psi^{-(r+1)}(w) + \beta$$

В скобках вида $\alpha^{-1}w(\dots)^t$ из разложения (5) коэффициент при w^{-k} и коэффициент при w^k, k — положительное, кратны β^k. Свободный член в той же скобке кратен β. Снова легко получаем соотношения

$$\begin{aligned} c_k^{r+2} &= 0 \pmod{\beta^{k-1}}, \quad k = 3, \dots, m \\ c_{-k}^{r+2} &= 0 \pmod{\beta^{k+1}}, \quad k = 1, \dots, m-2 \\ B^{r+2} &= 0 \pmod{\beta}. \end{aligned}$$

Подсчитываем c_1^{r+2}, c_2^{r+2}

$$c_1^{r+2} = \alpha(\alpha^{-1} - \alpha^{-2}(c_{-1}^{r+1} - \alpha)) = 1 \pmod{\beta^2}$$

$$c_2^{r+2} = \alpha(-\alpha^{-2}B^{r+1}) = -\frac{r+2}{2}\alpha^{-1}\beta \pmod{\beta^2}$$

Таким образом, теорема доказана. □

В дальнейшем нам еще понадобится следующая лемма.

Лемма 1. *Пусть* $\mathfrak{p} \in \mathbb{Z}[i]$ *— простое Гауссово число.* $F(x) \in \mathbb{Z}[i][x]$ *многочлен следующего вида:*

$$F(x) = \alpha_1 x + \alpha_2 x^2 + \ldots + \alpha_n x^n$$

$$\begin{aligned} \alpha_2 &\neq 0 \pmod{\mathfrak{p}} \\ \alpha_k &= 0 \pmod{\mathfrak{p}} \quad k = 3, \ldots, n \end{aligned}$$

Обозначим

$$S = \sum_{x \in \mathbb{Z}_{\mathfrak{p}^m}[i]} \exp\left(2\pi i Sp \frac{F(x)}{\mathfrak{p}^m}\right).$$

Тогда

$$|S| = N(\mathfrak{p}^{m/2}).$$

Доказательство. Делаем замену $x = y + \mathfrak{p}^{m-1} z$

$$S = \sum_{y \in \mathbb{Z}_{\mathfrak{p}^{m-1}}[i]} \exp\left(2\pi i Sp \frac{F(y)}{\mathfrak{p}^m}\right) \sum_{z \in \mathbb{Z}_{\mathfrak{p}}[i]} \exp\left(2\pi i Sp \frac{(\alpha_1 + 2\alpha_2 y)\mathfrak{p}^{m-1} z}{\mathfrak{p}^m}\right)$$

Известно, что сумма по z равна $N(\mathfrak{p})$, если $\alpha_1 + 2\alpha_2 y = 0 \pmod{\mathfrak{p}}$, и равна нулю в противном случае. Обозначим через y_0 решение сравнения $\alpha_1 + 2\alpha_2 y = 0 \pmod{\mathfrak{p}}$. Тогда

$$S = N(\mathfrak{p}) \sum_{\substack{y \in \mathbb{Z}_{\mathfrak{p}^{m-1}}[i] \\ \alpha_1 + 2\alpha_2 y = 0}} \exp\left(2\pi i Sp \frac{F(y)}{\mathfrak{p}^m}\right) = N(\mathfrak{p}) \sum_{t \in \mathbb{Z}_{\mathfrak{p}^{m-2}}[i]} \exp\left(2\pi i Sp \frac{F(y_0 + \mathfrak{p}t)}{\mathfrak{p}^m}\right) =$$

$$= N(\mathfrak{p}) \exp\left(2\pi i Sp \frac{F(y_0)}{\mathfrak{p}^m}\right) \sum_{t \in \mathbb{Z}_{\mathfrak{p}^{m-2}}[i]} \exp\left(2\pi i Sp \frac{\alpha_1 \mathfrak{p} t + 2\alpha_2 y_0 \mathfrak{p} t + \alpha_2 \mathfrak{p}^2 t^2 + \ldots}{\mathfrak{p}^m}\right)$$

Учитывая, что $\alpha_1 \mathfrak{p} + 2\alpha_2 y_0 \mathfrak{p} = 0 \pmod{\mathfrak{p}^2}$, можно записать

$$S = N(\mathfrak{p}) \exp\left(2\pi i Sp \frac{F(y_0)}{\mathfrak{p}^m}\right) \sum_{t \in \mathbb{Z}_{\mathfrak{p}^{m-2}}[i]} \exp\left(2\pi i Sp \frac{p^2 F_1(t)}{\mathfrak{p}^m}\right),$$

где

$$\begin{aligned} F_1(t) &= \beta_1 t + \beta_2 t^2 + \ldots + \beta_n t^n \\ \beta_2 &= \alpha_2 \neq 0 \pmod{\mathfrak{p}} \\ \beta_i &= 0 \pmod{\mathfrak{p}} \qquad i = 3, \ldots, n \end{aligned}$$

Рассмотрим случай четного m. Тогда, проделывая последовательно указанную выше процедуру, получим

$$S = N(\mathfrak{p}^{m/2}) \exp\left(2\pi i Sp \left(\frac{F(y_0)}{\mathfrak{p}^m} + \frac{F_1(t_0)}{\mathfrak{p}^m} + \ldots\right)\right).$$

Значит, в этом случае $|S| = N(\mathfrak{p}^{m/2})$.

Пусть m — нечетное. Проделывая последовательно ту же операцию и учитывая, что все коэффициенты получающихся многочленов, кроме 1-го и 2-го, кратны $\mathfrak{p}$, получим

$$S = N(\mathfrak{p}^{(m-1)/2}) \exp\left(2\pi i Sp\left(\frac{F(y_0)}{\mathfrak{p}^m} + \frac{F_1(t_0)}{\mathfrak{p}^m} + \dots\right)\right) \times \\ \times \sum_{u \in \mathbb{Z}_{\mathfrak{p}}[i]} \exp\left(2\pi i Sp \frac{cu + \alpha_2 u^2}{\mathfrak{p}}\right).$$

Сумма по u является суммой Гаусса и так как $(\alpha_2, \mathfrak{p}) = 1$ она равна $N(\mathfrak{p}^{1/2})$. В итоге получаем, $|S| = N(\mathfrak{p}^{(m-1)/2})N(\mathfrak{p}^{1/2}) = N(\mathfrak{p}^{m/2})$ $\square$

2. Оценка σ_r.

Обозначим через σ_r следующую тригонометрическую сумму

$$\sigma_r = \sum_{w \in \mathbb{Z}^*_{\mathfrak{p}^m}[i]} \exp\left(2\pi i Sp\left(h\frac{\psi^r(w) - w}{\mathfrak{p}^m}\right)\right),$$

здесь h — произвольный элемент из $\mathbb{Z}_{\mathfrak{p}^m}$.

Теорема 2. *Пусть* $h = \mathfrak{p}^d h_0$, $(h_0, \mathfrak{p}) = 1$, $0 \le d \le m-1$, $\beta = \mathfrak{p}^b \beta_1$, $(\beta_1, \mathfrak{p}) = 1$, $1 \le b \le m$. *Тогда*

$$|\sigma_r| \le 2N(\mathfrak{p})^{(m+d+b+\varepsilon)/2}, \quad \varepsilon = \begin{cases} 0 & \text{если} \quad m-d-b - \text{четное} \\ 1 & \text{если} \quad m-d-b - \text{нечетное} \end{cases}$$

Доказательство. При $d+b \ge m$ утверждение теоремы является следствием тривиальной оценки σ_r и мы будем считать $d + b < m$.

Сократим на $\mathfrak{p}^d$ числитель и знаменатель в показателе экспоненты.

$$\sigma_r = N(\mathfrak{p})^d \sum_{w \in \mathbb{Z}^*_{\mathfrak{p}^{m-d}}[i]} \exp\left(2\pi i Sp\left(h_0\frac{\psi^r(w) - w}{\mathfrak{p}^{m-d}}\right)\right).$$

Рассмотрим отдельно случай нечетного и четного r.

Пусть r — нечетное. Делаем замену $w = u + \mathfrak{p}^{m-d-1}v$, $u \in \mathbb{Z}^*_{\mathfrak{p}^{m-d-1}}[i]$, $v \in \mathbb{Z}_{\mathfrak{p}}[i]$, $w^{-1} = u^{-1}(1 - \mathfrak{p}^{m-d-1}vu^{-1})$

$$\psi^r(w) - w = (c_1^r - 1)(u + \mathfrak{p}^{m-d-1}v) + c_2^r + \dots + c_{m-2}^r + B^r + \\ + c_{-1}^r u^{-1}(1 - \mathfrak{p}^{m-d-1}vu^{-1}) + c_{-2}^r + \dots + c_{-m}^r u^{-m} = \\ = (\psi^r(u) - u) - \mathfrak{p}^{m-d-1}v - c_{-1}^r u^{-2}\mathfrak{p}^{m-d-1}v.$$

Значит,

$$\sigma_r = N(\mathfrak{p})^d \sum_{u \in \mathbb{Z}^*_{\mathfrak{p}^{m-d-1}}[i]} \exp\left(2\pi i Sp\left(h_0\frac{\psi^r(u) - u}{\mathfrak{p}^{m-d}}\right)\right) \times \\ \times \sum_{v \in \mathbb{Z}_{\mathfrak{p}}[i]} \exp\left(2\pi i Sp\left(-h_0\frac{(1 + c_{-1}^r u^{-2})v}{\mathfrak{p}}\right)\right).$$

Внутренняя сумма по v равна $N(\mathfrak{p})$, если $h_0(1+c_{-1}^r u^{-2}) = 0 \pmod{\mathfrak{p}}$ или, что то же самое, $u^2+\alpha = 0 \pmod{\mathfrak{p}}$. Во всех остальных случая она равна 0.

$$\sigma_r = N(\mathfrak{p})^{d+1} \sum_{\substack{u \in \mathbb{Z}^*_{\mathfrak{p}^{m-d-1}}[i] \\ u^2+\alpha = 0(\mathfrak{p})}} \exp\left(2\pi i Sp\left(h_0 \frac{\psi^r(u)-u}{\mathfrak{p}^{m-d}}\right)\right) \tag{6}$$

Предположим, сравнение $u^2+\alpha = 0 \pmod{\mathfrak{p}}$ имеет решение в $\mathbb{Z}^*_{\mathfrak{p}}[i]$ и u_0 одно из таких решений.

Рассмотрим $\sum\limits_{z \in \mathbb{Z}_{\mathfrak{p}^{m-d-2}}[i]} \exp\left(2\pi i Sp\left(h_0 \frac{\psi^r(u_0+\mathfrak{p}z)-(u_0+\mathfrak{p}z)}{\mathfrak{p}^{m-d}}\right)\right)$.

$$(u_0+\mathfrak{p}z)^{-1} = u_0^{-1} - \mathfrak{p}z u_0^{-2} + \mathfrak{p}^2 z^2 u_0^{-3} - \ldots + (-1)^{m-d-1}\mathfrak{p}^{m-d-1} z^{m-d-1} u_0^{-(m-d)};$$

$$\begin{aligned}
\psi^r(u_0+\mathfrak{p}z) - (u_0+\mathfrak{p}z) = \\
&= (c_1^r - 1)(u_0+\mathfrak{p}z) + c_2^r(u_0+\mathfrak{p}z)^2 + \ldots + c_{m-2}^r(u_0+\mathfrak{p}z)^{m-2} + B^r + \\
&+ c_{-1}^r(u_0^{-1} - \mathfrak{p}z u_0^{-2} + \ldots + (-1)^{m-d-1}\mathfrak{p}^{m-d-1} z^{m-d-1} u_0^{-(m-d)}) + \ldots + \\
&+ c_{-m}^r(u_0^{-1} - \mathfrak{p}z u_0^{-2} + \ldots + (-1)^{m-d-1}\mathfrak{p}^{m-d-1} z^{m-d-1} u_0^{-(m-d)})^m.
\end{aligned}$$

После раскрытия скобок и приведения подобных коэффициент при z будет кратен $\mathfrak{p}^2$, так как согласно теореме (1) все коэффициенты c_i, кроме c_{-1}, делятся на $\mathfrak{p}$, а $\mathfrak{p}z - c_{-1}^r \mathfrak{p} z u_0^{-2} = 0 \pmod{\mathfrak{p}^2}$. Коэффициент при z^2 дает остаток $\mathfrak{p}^2 c_{-1}^r = \mathfrak{p}^2\alpha$ при делении на $\mathfrak{p}^3$. Коэффициенты при остальных степенях z^i $i = 3, \ldots, m-1$, очевидно, кратны $\mathfrak{p}^i$. Значит,

$$\begin{aligned}
\psi^r(u_0+\mathfrak{p}z) - (u_0+\mathfrak{p}z) &= \psi^r(u_0) - u_0 + \mathfrak{p}^2 G(z) \\
G(z) &= \beta_1 z + \beta_2 z^2 + \ldots + b_{m-1} z^{m-1} \\
\beta_2 &= \alpha \pmod{\mathfrak{p}} \\
\beta_i &= 0 \pmod{\mathfrak{p}} \quad i = 3, \ldots, m-1.
\end{aligned}$$

Таким образом $h_0 G(z)$ удовлетворяет условиям леммы (1), и мы можем записать

$$\begin{aligned}
&\left| \sum_{z \in \mathbb{Z}_{\mathfrak{p}^{m-d-2}}[i]} \exp\left(2\pi i Sp\left(h_0 \frac{\psi^r(u_0+\mathfrak{p}z)-(u_0+\mathfrak{p}z)}{\mathfrak{p}^{m-d}}\right)\right)\right| = \\
&= \left| \exp\left(2\pi i Sp \frac{h_0(\psi^r(u_0)-u_0)}{\mathfrak{p}^m}\right) \sum_{z \in \mathbb{Z}_{\mathfrak{p}^{m-d-2}}} \exp\left(2\pi i Sp \frac{h_0 G(z)}{\mathfrak{p}^{m-d-2}}\right)\right| = \\
&= N(\mathfrak{p})^{(m-d-2)/2}
\end{aligned}$$

Сравнение $u^2+\alpha = 0 \pmod{\mathfrak{p}}$ может иметь максимум 2 решения, лежащих в $\mathbb{Z}^*_{\mathfrak{p}}[i]$, и из (6) получаем $|\sigma_r| \le 2N(\mathfrak{p})^{p+1} N(\mathfrak{p})^{(m-d-2)/2} = 2N(\mathfrak{p})^{(m+d)/2}$. Тем самым для нечетного случая теорема доказана.

Пусть r — четное. Согласно теореме (1), в этом случае все коэффициенты $\psi^r(w) - w$ делятся на β.

$$\psi^r(w) - w = \mathfrak{p}^b(\mathfrak{p}^{-b}(c_1^r - 1)w + \mathfrak{p}^{-b}c_2^r w^2 + \ldots + \mathfrak{p}^{-b}c_m^r w^m + \mathfrak{p}^{-b}B^r + \\ + \mathfrak{p}^{-b}c_{-1}^r + \ldots + \mathfrak{p}^{-b}c_{-(m-2)}^r w^{-(m-2)}).$$

Обозначим $m_1 = m - d - b$ и рассмотрим случай $m_1 = 2g$. Сделаем замену $w = u + \mathfrak{p}^g v$, $u \in \mathbb{Z}_{\mathfrak{p}^g}^*[i]$, $v \in \mathbb{Z}_{\mathfrak{p}^g}[i]$, $w^{-1} = u^{-1}(1 - \mathfrak{p}^g v u^{-1})$.

$$\begin{aligned}
&\mathfrak{p}^{-b}(\psi^r(w) - w) = \\
&= \mathfrak{p}^{-b}(c_1^r - 1)(u + \mathfrak{p}^g v) + \mathfrak{p}^{-b}c_2^r(u^2 + 2\mathfrak{p}^g vu) + \ldots + \mathfrak{p}^{-b}c_m^r(u^m + m\mathfrak{p}^g v u^{m-1}) + \\
&+ \mathfrak{p}^{-b}B^r + \mathfrak{p}^{-b}c_{-1}^r(u^{-1} - \mathfrak{p}^g v u^{-2}) + \\
&+ \mathfrak{p}^{-b}c_{-2}^r(u^{-2} - 2\mathfrak{p}^g v u^{-3}) + \ldots + \mathfrak{p}^{-b}c_{-(m-2)}^r(u^{-(m-2)} + (m-2)\mathfrak{p}^g v u^{-(m-1)}) = \\
&= \mathfrak{p}^{-b}(\psi^r(u) - u) + \mathfrak{p}^g v\Phi(u).
\end{aligned}$$

Здесь $\Phi(u) = \mathfrak{p}^{-b}(c_1^r - 1) + 2\mathfrak{p}^{-b}c_2^r u + \ldots$. Покажем, что сравнение $\Phi(u) = 0 \pmod{\mathfrak{p}^g}$ имеет ровно одно решение (необязательно принадлежащее $\mathbb{Z}_{\mathfrak{p}^g}^*$). Рассмотрим $\Phi(u) = 0 \pmod{\mathfrak{p}}$. Согласно теореме (1) последнее сравнение эквивалентно $-r\alpha^{-1}b_1 u = 0 \pmod{\mathfrak{p}}$, откуда очевидно следует существование решения $u = 0$ по модулю $\mathfrak{p}$. Делая замену $u = pu_1 \pmod{\mathfrak{p}^2}$, раскладывая $\Phi(u)$ в ряд Тейлора в окрестности точки 0 и учитывая, что $\Phi'(u) \neq 0 \pmod{\mathfrak{p}}$, получим единственность решения по модулю $\mathfrak{p}^2$. Продолжая аналогично, получим единственность решения сравнения по модулю $\mathfrak{p}^g$.

Запишем окончательную оценку σ_r для r и m_1 — четных.

$$\begin{aligned}
|\sigma_r| &= N(\mathfrak{p})^{d+b}\left|\sum_{w \in \mathbb{Z}_{\mathfrak{p}^{m_1}}^*[i]} \exp\left(2\pi i Sp\left(h_0\frac{\mathfrak{p}^{-b}(\psi^r(w) - w)}{\mathfrak{p}^{m_1}}\right)\right)\right| = \\
&= N(\mathfrak{p})^{d+b}\left|\sum_{u \in \mathbb{Z}_{\mathfrak{p}^g}^*[i]} \exp\left(2\pi i Sp\left(h_0\frac{\mathfrak{p}^{-b}(\psi^r(u) - u)}{\mathfrak{p}^{m_1}}\right)\right)\cdot\right. \\
&\left.\cdot \sum_{v \in \mathbb{Z}_{\mathfrak{p}^g}[i]} \exp\left(2\pi i Sp\left(h_0\frac{\Phi(u)v}{\mathfrak{p}^g}\right)\right)\right| = \\
&= N(\mathfrak{p})^{d+b+g}\left|\sum_{\substack{u \in \mathbb{Z}_{\mathfrak{p}^g}^*[i] \\ \Phi(u) = 0(\mathfrak{p}^g)}} \exp\left(2\pi i Sp\left(h_0\frac{\mathfrak{p}^{-b}(\psi^r(u) - u)}{\mathfrak{p}^{m_1}}\right)\right)\right| \leq \\
&\leq N(\mathfrak{p})^{d+b+g} = N(\mathfrak{p})^{(m+d+b)/2}.
\end{aligned}$$

Пусть $m_1 = 2g+1$. Используем замену $w = u + \mathfrak{p}^g v + \mathfrak{p}^{g+1}t$, $t \in \mathbb{Z}_{p^g}[i]$, $v \in \mathbb{Z}_p[i]$,

$u \in \mathbb{Z}^*_{p^g}[i]$, $w^{-1} = u^{-1}(1 - u^{-1}\mathfrak{p}^g v - u^{-1}\mathfrak{p}^{g+1}t + u^{-2}\mathfrak{p}^{2g}v^2)$;

$$w^k = u^k + k\mathfrak{p}^g v u^{k-1} + k\mathfrak{p}^{g+1}tu^{k-1} + \frac{k(k-1)}{2}\mathfrak{p}^{2g}v^2u^{k-2};$$

$$w^{-k} = u^{-k} - ku^{-(k+1)}\mathfrak{p}^g v - ku^{-(k+1)}\mathfrak{p}^{g+1}t + ku^{-(k+2)}\mathfrak{p}^{2g}v^2 + \frac{k(k-1)}{2}u^{-(k+2)}\mathfrak{p}^{2g}v^2;$$

$$\mathfrak{p}^{-b}(\psi^r(w) - w) = \mathfrak{p}^{-b}(\psi^r(w) - w) + \mathfrak{p}^{g+1}t(\mathfrak{p}^{-b}(c_1^r - 1)u + \mathfrak{p}^{-b}2c_2^r u + \ldots +$$
$$+ \mathfrak{p}^{-b}mc_m^r u^{m-1} - \mathfrak{p}^{-b}c_{-1}^r u^{-2} - \mathfrak{p}^{-b}2c_{-2}^r u^{-3} - \ldots - \mathfrak{p}^{-b}(m-2)c_{-(m-2)}^r u^{-(m-1)}) +$$
$$+ \mathfrak{p}^g v(\ldots) + \mathfrak{p}^{2g}v^2(\ldots) = \mathfrak{p}^{-b}(\psi^r(w) - w) + \mathfrak{p}^{g+1}t\Phi(u) + \mathfrak{p}^g v(\ldots) + \mathfrak{p}^{2g}v^2(\ldots);$$

$$|\sigma^r| = N(\mathfrak{p})^{d+b}\left|\sum_{u \in \mathbb{Z}^*_{\mathfrak{p}^g}[i]} \exp\left(2\pi i Sp\left(h_0\frac{\mathfrak{p}^{-b}(\psi^r(u) - u)}{\mathfrak{p}^{m_1}}\right)\right) \times\right.$$

$$\left.\times \sum_{t \in \mathbb{Z}_{\mathfrak{p}^g}[i]} \exp\left(2\pi i Sp\left(h_0\frac{\Phi(u)t}{\mathfrak{p}^g}\right)\right) \sum_{v \in \mathbb{Z}_{\mathfrak{p}}[i]} \exp\left(2\pi i Sp\left(h_0\frac{\mathfrak{p}^g v(\ldots) + \mathfrak{p}^{2g}v^2(\ldots)}{\mathfrak{p}^{m_1}}\right)\right)\right|.$$

Сумму по v оцениваем тривиально, $N(\mathfrak{p})$. Оставшиеся суммы по u и t аналогичны случаю $m_1 = 2g$, а значит, $|\sigma_r| \le N(\mathfrak{p})^{d+b}N(\mathfrak{p})N(\mathfrak{p})^g = N(\mathfrak{p})^{(m+b+d+1)/2}$, что завершает доказательство теоремы. □

3. Оценка $S_h(M)$

Введем в рассмотрение следующую сумму

$$S_h(M) = \sum_{n=0}^{M-1} \exp\left(2\pi i Sp\left(\frac{hw_n}{\mathfrak{p}^m}\right)\right).$$

Теорема 3. *Представим h и β в виде $h = \mathfrak{p}^d h_0$, $(h_0, \mathfrak{p}) = 1$, $0 \le d \le m-1$, $\beta = \mathfrak{p}^b\beta_1$, $(\beta_1, \mathfrak{p}) = 1$, $1 \le b \le m$.*

Тогда

$$|S_h(M)| < 2.16M^{1/2}N(\mathfrak{p})^{(m+d+b+\varepsilon)/4}, \quad \varepsilon = \begin{cases} 0 & \text{если } m-d-b \text{ — четное} \\ 1 & \text{если } m-d-b \text{ — нечетное} \end{cases}$$

Доказательство. По определению, $w_n = \psi^n(w_0)$ для всех $n \ge 0$. Используем это соотношение для определения u_n при отрицательных n. Тогда для любого $k \in \mathbb{Z}$

$$\left|S_h(M) - \sum_{n=0}^{M-1} \exp\left(2\pi i Sp\left(\frac{hw_{n+k}}{\mathfrak{p}^m}\right)\right)\right| \le 2|k| \tag{7}$$

Для $K \ge 1$ положим

$$R(K) = \begin{cases} \{k \in \mathbb{Z} | -(K-1)/2 \le k \le (K-1)/2\} & \text{если } K \text{ — нечетное} \\ \{k \in \mathbb{Z} | -K/2 \le k \le K/2\} & \text{если } K \text{ — четное} \end{cases}$$

Легко проверить, что

$$\sum_{k \in R(K)} |k| \le K^2/4$$

Записав (7) для каждого $k \in R(K)$, сложив полученные неравенства и проделав тривиальные преобразования, можно получить

$$K|S_h(M)| \le W + K^2/2, \tag{8}$$

где

$$W = \left| \sum_{n=0}^{M-1} \sum_{k \in R(K)} \exp\left(2\pi i Sp\left(\frac{hw_{n+k}}{\mathfrak{p}^m}\right)\right)\right| \le \sum_{n=0}^{M-1} \left| \sum_{k \in R(K)} \exp\left(2\pi i Sp\left(\frac{hw_{n+k}}{\mathfrak{p}^m}\right)\right)\right|.$$

Применим неравенство Коши–Буняковского

$$\begin{aligned}
W^2 &\le M \sum_{n=0}^{M-1} \left| \sum_{k \in R(K)} \exp\left(2\pi i Sp\left(\frac{hw_{n+k}}{\mathfrak{p}^m}\right)\right)\right|^2 = \\
&= M \sum_{n=0}^{M-1} \left| \sum_{k \in R(K)} \exp\left(2\pi i Sp\left(\frac{h\psi^k(w_n)}{\mathfrak{p}^m}\right)\right)\right|^2 \le \\
&\le M \sum_{w \in \mathbb{Z}^*_{\mathfrak{p}^m}[i]} \left| \sum_{k \in R(K)} \exp\left(2\pi i Sp\left(\frac{h\psi^k(w)}{\mathfrak{p}^m}\right)\right)\right|^2 \le \\
&\le M \sum_{k,l \in R(K)} \left| \sum_{w \in \mathbb{Z}^*_{\mathfrak{p}^m}[i]} \exp\left(2\pi i Sp\left(\frac{h(\psi^k(w) - \psi^l(w)}{\mathfrak{p}^m}\right)\right)\right| \le \\
&\le MKN(\mathfrak{p})^m + \sum_{\substack{k,l \in R(K) \\ k>l}} \left| \sum_{w \in \mathbb{Z}^*_{\mathfrak{p}^m}[i]} \exp\left(2\pi i Sp\left(\frac{h(\psi^k(w) - \psi^l(w)}{\mathfrak{p}^m}\right)\right)\right|.
\end{aligned}$$

Учитывая, что ψ — перестановка $\mathbb{Z}^*_{\mathfrak{p}^m}[i]$, запишем

$$\begin{aligned}
&\sum_{w \in \mathbb{Z}^*_{\mathfrak{p}^m}[i]} \exp\left(2\pi i Sp\left(\frac{h(\psi^k(w) - \psi^l(w)}{\mathfrak{p}^m}\right)\right) = \\
&= \sum_{w \in \mathbb{Z}^*_{\mathfrak{p}^m}[i]} \exp\left(2\pi i Sp\left(\frac{h(\psi^{k-l}(\psi^l(w)) - \psi^l(w)}{\mathfrak{p}^m}\right)\right) = \\
&= \sum_{w \in \mathbb{Z}^*_{\mathfrak{p}^m}[i]} \exp\left(2\pi i Sp\left(\frac{h(\psi^{k-l}(w) - w)}{\mathfrak{p}^m}\right)\right).
\end{aligned}$$

Так же запишем

$$W^2 \le MKN(\mathfrak{p})^m + 2M \sum_{r=1}^{K-1} (K-r)|\sigma_r|.$$

Применяем теорему (2).

$$W^2 \le MKN(\mathfrak{p})^m + 2M2N(\mathfrak{p})^{(m+d+b+\varepsilon)/2} \frac{K(K-1)}{2}$$

$$W \le M^{1/2}\left(KN(\mathfrak{p})^m + 2N(\mathfrak{p})^{(m+d+b+\varepsilon)/2}K(K-1)\right)^{1/2}$$

Подставляем полученную оценку для W в (8)

$$|S_h(M)| < \frac{K}{2} + M^{1/2}(K^{-1}N(\mathfrak{p})^m + 2N(\mathfrak{p})^{(m+d+b+\varepsilon)/2})^{1/2}$$

Положим

$$K = \lceil N(\mathfrak{p})^{(m-d-b-\varepsilon)/2}\rceil,$$

и оценка $|S_h(M)|$ примет вид

$$|S_h(M)| < \frac{1}{2}(N(\mathfrak{p})^{(m-d-b-\varepsilon)/2}+1) + \sqrt{3}M^{1/2}N(\mathfrak{p})^{(m+d+b+\varepsilon)/4} \tag{9}$$

Мы можем считать, что

$$M \ge 2.16^2 N(\mathfrak{p})^{m/2}, \tag{10}$$

потому что в противном случае

$$|S_h(M)| \le M^{1/2+1/2} < 2.16M^{1/2}N(\mathfrak{p})^{m/4}.$$

Из (10) следует $N(\mathfrak{p})^{m/2} \le \frac{1}{2.16}M^{1/2}N(\mathfrak{p})^{m/4}$ и $1 < 0.8N(\mathfrak{p})^{m/2}$ $\le \frac{0.8}{2.16}M^{1/2}N(\mathfrak{p})^{m/4}$. Значит, $N(\mathfrak{p})^{(m-d-b-\varepsilon)/2}+1 \le \frac{1.8}{2.16}M^{1/2}N(\mathfrak{p})^{m/4}$. С учетом этого из (9) легко следует утверждение теоремы. □

4. Оценка дискрепанции D_M

Теорема 4. *Для дискрепанции последовательности (2) справедлива оценка*

$$D_M \le M^{-1/2}N(\mathfrak{p})^{(m+b+\varepsilon)/4}(36.9 + 4.4\ln M)$$

ε такое же, как в теореме (2).

Доказательство. Для любого целого $H \ge 1$ известна оценка (см. [4])

$$D_M \le \frac{1}{H+1} + \frac{2}{N}\sum_{h=1}^{H}\left(\frac{1}{\pi h} + \frac{1}{H+1}\right)|S_h(M)|. \tag{11}$$

Пусть $\mathfrak{p}$ таково, что $N(\mathfrak{p}) = 4k+1$. Оценим

$$\sum_{\substack{h=1\\ \mathfrak{p}^d|h}}^{H}\frac{1}{h} = \sum_{\substack{h=1\\ N(\mathfrak{p})^d|h}}^{H}\frac{1}{h} = \frac{1}{N(\mathfrak{p})^d}\sum_{h=1}^{\left\lfloor\frac{H}{N(\mathfrak{p})^d}\right\rfloor}\frac{1}{H} \le \frac{1}{N(\mathfrak{p})^d}\left(1+\ln\frac{H}{N(\mathfrak{p})^d}\right) \le$$
$$\le \frac{1}{N(\mathfrak{p})^d}\left(1+\ln H\right).$$

Из теоремы (3) следует

$$\sum_{h=1}^{H}\frac{1}{h}|S_h(M)| < 2.16M^{1/2}N(\mathfrak{p})^{(m+b+\varepsilon)/4}\sum_{d=0}^{\infty}N(\mathfrak{p})^{d/4}\sum_{\substack{h=1\\ \mathfrak{p}^d|h}}^{H}\frac{1}{h} \le$$

$$\le 2.16M^{1/2}N(\mathfrak{p})^{(m+b+\varepsilon)/4}(1+\ln H)\sum_{d=0}^{\infty}N(\mathfrak{p})^{-3d/4} =$$

$$= 2.16M^{1/2}N(\mathfrak{p})^{(m+b+\varepsilon)/4}(1+\ln H)\frac{1}{1-N(\mathfrak{p})^{-3/4}} <$$

$$< 5.4M^{1/2}N(\mathfrak{p})^{(m+b+\varepsilon)/4}(1+\ln H).$$

Рассмотрение $\mathfrak{p}=4k+3$ происходит аналогично, и в этом случае получается

$$\sum_{h=1}^{H}\frac{1}{h}|S_h(M)| < 13.6M^{1/2}N(\mathfrak{p})^{(m+b+\varepsilon)/4}(1+\ln H), \tag{12}$$

значит, неравенство (12) выполняется для любого простого Гауссового $\mathfrak{p}$.

Аналогичным образом рассматривая 2 случая, для любого простого $\mathfrak{p}$ получим оценку

$$\sum_{h=1}^{H}|S_h(M)| < 13.6M^{1/2}N(\mathfrak{p})^{(m+b+\varepsilon)/4}H. \tag{13}$$

Подставляем оценки сумм (12) и (13) в (11)

$$D_M < \frac{1}{H+1} + 27.2M^{-1/2}N(\mathfrak{p})^{(m+b+\varepsilon)/4}\left(\frac{1}{\pi}(1+\ln H)+1\right).$$

Выбираем H равным

$$H = \left\lfloor M^{1/2}N(\mathfrak{p})^{(m+b+\varepsilon)/4}\right\rfloor,$$

тогда

$$D_M < M^{-1/2}N(\mathfrak{p})^{(m+b+\varepsilon)/4} +$$

$$+ 27.2M^{-1/2}N(\mathfrak{p})^{(m+b+\varepsilon)/4}\left(\frac{1}{\pi}\left(1+\frac{1}{2}\ln M - \frac{m+b+\varepsilon}{4}\ln N(\mathfrak{p})\right)+1\right) \le$$

$$\le M^{-1/2}N(\mathfrak{p})^{(m+b+\varepsilon)/4}\left(1+27.2+\frac{27.2}{\pi}+\frac{27.2}{2\pi}\ln M.\right).$$

Тем самым получаем требуемое. □

Полученная оценка не является тривиальной, если M по порядку больше, чем $N(\mathfrak{p})^{(m+b+\varepsilon)/2}\ln^2 N(\mathfrak{p})$.

Заключение. Полученная оценка дискрепанции говорит о том, что последовательность (2) равномерно распределена на отрезке $[0,1]$. Использование указанной последовательности в методах Монте-Карло и криптографических приложениях может привести к лучшем результатам, чем использование этих методов с иными последовательностями псевдослучайных чисел.

1. **H. Niederreiter** On the distribution of inversive congruential pseudorandom numbers in parts of the period [text] / H. Niederreiter, I. E. Shparlinski // Math. Comput. – 2001. – P. 1569–1574.
2. **H. Niederreiter** Exponential sums and the distribution of inversive congruential pseudorandom numbers with prime-power modulus [text] / H. Niederreiter, I. E. Shparlinski // Acta Arith. – V. 92. – P. 89–98.
3. **S. Varbanets** On inversive congruential generator for pseudorandom numbers with prime power modulus [text] / S. Varbanets // Annales Univ. Sci. Budapest., Sect. Comp 29. – 2008. – P. 277–296.
4. **J. D. Vaaler** Some extremal functions in Fourier analysis [text] / J. D. Vaaler // Bull. Amer. Math. Soc. – 1985. – P. 183–216.
5. **M. Flahive** On inversive congruential generators for pseudorandom numbers [text] / M. Flahive, H. Niederreiter // Finite Fields, Coding Theory, and Advances in Communications and Computing. – New York. – 1993. – P. 75–80.
6. **J. Eichenauer-Herrmann** A survey of quadratic and inversive congruential pseudorandom numbers [text] / J. Eichenauer-Herrmann, E. Herrmann, S. Wegenkittl // Lect. Notes in Statistics 127. – Springer-Verlag, Berlin. – 1998. – P. 66–97.
7. **R. Lidl** Finite Fields and their applications [text] / R. Lidl, H. Niederreiter. – Elsevier, Amsterdam. – 1996. – P. 321–363.
8. **H. Niederreiter** The serial test for congruential pseudorandom numbers generated by inversions [text] / H. Niederreiter // Math. Comp. 52. – 1989. – P. 135–144.
9. **H. Niederreiter** Random number generation and quasi-Monte Carlo methods [text] / H. Niederreiter. – SIAM, Philadelphia. – 1992.
10. **H. Niederreiter** Finite Fields, pseudorandom numbers, and quasirandom points [text] / H. Niederreiter // Finite Fields, Coding Theory, and Advances in Communications and Computing. – New York. – 1993 – P. 375–394.
11. **H. Niederreiter** New developments in uniform pseudorandom number and vector generation [text] / H. Niederreiter // Lect. Notes in Statistics 106. – Springer-Verlag, Berlin. – 1995. – P. 87–120.