Вісник Одеськ. нац. ун-ту. Матем. і мех. – 2010. – Т. 15, вип. 19. – С. 62–76

УДК 511.32

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

ИНВЕРСНЫЙ КОНГРУЕНТНЫЙ ГЕНЕРАТОР С ПЕРЕМЕННЫМ СДВИГОМ НАД КОЛЬЦОМ ЦЕЛЫХ ГАУССОВЫХ ЧИСЕЛ

Задорожний С. О. Інверсний конгруентний генератор із змінним зсувом над кільцем цілих гауссових чисел. В даній роботі розглядається генератор $\psi_{r+1}(w) \equiv \alpha\psi_r^{-1}(w) + \beta + \gamma(r+1)w \pmod{\mathfrak{p}^m}$ над кільцем цілих гауссових чисел, знаходиться його період та отримуються дві оцінки для дискрепанції: у середньому по всіх w та для індивідуального значення w.
Ключові слова: дискрепанція, інверсний конгруентальний метод, числа Гаусса, тригонометрична сума.

Задорожный С. А. Инверсный конгруентный генератор с переменным сдвигом над кольцом целых гауссовых чисел. В данной работе рассматривается генератор $\psi_{r+1}(w) \equiv \alpha\psi_r^{-1}(w) + \beta + \gamma(r+1)w \pmod{\mathfrak{p}^m}$ над кольцом целых гауссовых чисел, находится его период и получаются две оценки для дискрепанции: в среднем по всем w и для индивидуального значения w.
Ключевые слова: дискрепанция, инверсный конгруентальный метод, числа Гаусса, тригонометрическая сумма.

Zadorozhny S. A. Inversive congruential generator with variable shift over the ring of Gaussian integers. In this paper the generator $\psi_{r+1}(w) \equiv \alpha\psi_r^{-1}(w) + \beta + \gamma(r+1)w \pmod{\mathfrak{p}^m}$ is considered. Its period is found and two discrepancy bounds are obtained, one is on average over all w, another one is for individual value of w.
Key words: discrepancy, inversive congruential method, gaussian numbers, exponential sum.

Введение.

Последовательности случайных чисел, обладающие свойством равномерной распределенности и непредсказуемости, имеют различные приложения в задачах моделирования (метод Монте-Карло) и в криптографии (при генерировании случайных ключей). Поскольку случайные числа мы строить не умеем, на практике используются псевдослучайные числа, которые по основным характеристикам похожи на случайные. Оказалось, что проще всего генерировать конгруэнтные псевдослучайные числа, которые обычно задаются рекурсивно.

$$y_{n+1} \equiv f(y_0, \dots, y_n) \pmod{M},$$

где f — целозначная функция.

Наиболее изученным является инверсный конгруэнтный генератор вида

$$y_{n+1} \equiv \frac{a}{y_n} + b \pmod{M},$$

где M — есть степень простого. Параметры a, b и инициальное значение y_0 выбираются так, чтобы рекурсия не имела остановки. В этом случае мы полу-

чим последовательность псевдослучайных чисел не превосходящих M. Последовательность псевдослучайных чисел отрезка $[0,1]$ получается нормированием y_n/M.

Такого рода генератор и его обобщения изучались в работах Лехна, Эйченауэра, Топузоглу, Нидеррайтера, Шпарлинского (см. [1] [2], [3], [6]–[10]). В настоящей работе мы переносим методы генерирования псевдослучайных чисел над $\mathbb{Z}$ на $\mathbb{Z}[i]$.

Пусть $\mathfrak{p}$ — простое гауссово число, $m \in \mathbb{N}$, $m \geq 2$. Введем в рассмотрение отображения $\psi_r(w)$, строящиеся рекуррентно.

$$\begin{aligned} \psi_0(w) &= w, \\ \psi_{r+1}(w) &\equiv \alpha\psi_r^{-1}(w) + \beta + \gamma(r+1)w \pmod{\mathfrak{p}^m}, \end{aligned} \tag{1}$$

здесь $\alpha \in \mathbb{Z}^*_{\mathfrak{p}^m}$, $\beta, \gamma \in \mathbb{Z}_{\mathfrak{p}^m}$, $\beta \equiv 0 \pmod{\mathfrak{p}}$, $\gamma \equiv 0 \pmod{\mathfrak{p}}$. $\psi_r^{-1}(w)$ есть мультипликативно-обратное к $\psi_r(w)$ по модулю $\mathfrak{p}^m$, $\psi_r^{-1}(w) \cdot \psi_r(w) \equiv 1 \pmod{\mathfrak{p}^m}$. При выбранных α, β, γ $\psi_r(w)$ является отображением $\mathbb{Z}^*_{\mathfrak{p}^m} \to \mathbb{Z}^*_{\mathfrak{p}^m}$ для любого $r \geq 0$.

Если зафиксируем w $(w, \mathfrak{p}) = 1$, то получим последовательность комплексных чисел:

$$\psi_0(w), \quad \psi_1(w), \quad \psi_2(w), \quad \ldots \tag{2}$$

которая в свою очередь определяет следующую последовательность действительных чисел полуинтервала $[0,1)$:

$$\left\{Re\left(\frac{\psi_0(w)}{\mathfrak{p}^m}\right)\right\}, \quad \left\{Re\left(\frac{\psi_1(w)}{\mathfrak{p}^m}\right)\right\}, \quad \left\{Re\left(\frac{\psi_2(w)}{\mathfrak{p}^m}\right)\right\}, \quad \ldots \tag{3}$$

Определим дискрепанцию $D_M(w)$ последовательности (3) как

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

где супремум берется по всем подынтервалам J полуинтервала $[0,1)$, $A(J,M)$ — количество точек $\{Re\,(\psi_r(w)/\mathfrak{p}^m)\}$, $0 \leq r \leq M-1$, попавших в интервал J, $|J|$ — длина интервала J.

Генератор, содержащий в себе черты инверсного и линейного генератора, был рассмотрен С. П. Варбанцом в [4]. Мы обобщаем генератор Варбанца и рассматриваем его над кольцом целых гауссовых чисел. Данная работа посвящена исследованию последовательностей (2) и (3). Мы находим период последовательности (2) и получаем две оценки сверху для дискрепанции последовательности (3). Одна оценка в среднем по всем w, вторая — для индивидуального значения w.

Обозначения. Обозначим через $\mathbb{Z}[i]$ кольцо целых гауссовых чисел $\mathbb{Z}[i] = \{a+bi \mid a,b \in \mathbb{Z},\ i^2=-1\}$. Через $\mathfrak{p}$ будем обозначать простое гауссово число, через p — простое рациональное. Через $\mathbb{Z}_{\mathfrak{p}^m}[i]$ будем обозначать полную систему гауссовых чисел по модулю $\mathfrak{p}^m$, а через $\mathbb{Z}^*_{\mathfrak{p}^m}[i]$ — приведенную систему гауссовых чисел. Через (a,b) будем записывать наибольший общий делитель чисел a, b.

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

В некоторых теоремах мы будем различать 2 случая простого гауссового $\mathfrak{p}$. Первый случай, $(\mathfrak{p},\bar{\mathfrak{p}})=\mathfrak{p}$. В этом случае $\mathfrak{p}$ является также простым рациональным числом вида $4k+3$. Второй случай, $(\mathfrak{p},\bar{\mathfrak{p}})=1$. Здесь $Re(\mathfrak{p})\neq 1$, $Im(\mathfrak{p})\neq 1$ и $\bar{\mathfrak{p}}$ также является простым гауссовым. Норма $N(\mathfrak{p})$ есть простое рациональное число вида $4k+1$.

Основные результаты.

1. Представления $\psi_r(w)$.

Лемма 1. *Пусть $\beta=\mathfrak{p}^b\beta_0$, $(\beta_0,\mathfrak{p})=1$, $1\le b\le m-1$, $\gamma=\mathfrak{p}^c\gamma_0$, $(\gamma_0,\mathfrak{p})=1$, $1\le c\le m-1$. При этом $b<c$. Тогда для любого $r\ge 0$*

$$\psi_r(w)=\frac{A_0^r+A_1^rw+\ldots+A_r^rw^r+A_{r+1}^rw^{r+1}}{B_0^r+B_1^rw+\ldots+B_r^rw^r},$$

где

$$B_i^r=A_i^{r-1},\quad i=1,\ldots r.$$

Для r-четного

$$A_0^r\equiv\frac{r}{2}\alpha^{r/2}\beta\pmod{\mathfrak{p}^{2b}}\qquad A_1^r\equiv\alpha^{r/2}\left(1+\frac{r}{2}\cdot\frac{r+2}{2}\gamma\right)\pmod{\mathfrak{p}^{2b}},$$
$$A_{2k}^r\equiv 0\pmod{\mathfrak{p}^{2kb}}\quad k=1,\ldots,r/2,$$
$$A_{2k+1}^r\equiv 0\pmod{\mathfrak{p}^{2kb}}\quad k=1,\ldots,r/2.$$

Для r-нечетного

$$A_0^r\equiv\alpha^{(r+1)/2}\pmod{\mathfrak{p}^{2b}}\qquad A_1^r\equiv\frac{r+1}{2}\alpha^{(r-1)/2}\beta\pmod{\mathfrak{p}^{2b}},$$
$$A_2^r\equiv\left(\frac{r+1}{2}\right)^2\alpha^{(r-1)/2}\gamma\pmod{\mathfrak{p}^{2b}},$$
$$A_{2k}^r\equiv 0\pmod{\mathfrak{p}^{(2k-1)b}}\quad k=2,\ldots,(r+1)/2,$$
$$A_{2k+1}^r\equiv 0\pmod{\mathfrak{p}^{(2k+1)b}}\quad k=1,\ldots,(r-1)/2.$$

Доказательство. Доказательство легко проводится индукцией по r. □

Следствие. *Период последовательности (2) есть четное число, если $w^2\not\equiv\alpha\pmod{\mathfrak{p}^b}$.*

Доказательство. Пусть r — четное. Тогда

$$\psi_r(w)\equiv\frac{\alpha^{r/2}w}{\alpha^{r/2}}\equiv w\pmod{\mathfrak{p}^b}.$$

Пусть r — нечетное.

$$\psi_r(w)\equiv\frac{\alpha^{(r+1)/2}w}{\alpha^{(r-1)/2}}\equiv\frac{\alpha}{w}\pmod{\mathfrak{p}^b}.$$

Если период последовательности (2) — нечетное число, то для некоторых t и s $\psi_{2t}(w)=\psi_{2s+1}(w)$, а значит, $w\equiv\alpha/w\pmod{\mathfrak{p}^b}$ и $w^2\equiv\alpha\pmod{\mathfrak{p}^b}$, что противоречит условию теоремы.

□

Теорема 1. *Пусть* $\beta = \mathfrak{p}^b\beta_0$, $(\beta_0, \mathfrak{p}) = 1$, $1 \le b \le m-1$, $\gamma = \mathfrak{p}^c\gamma_0$, $(\gamma_0, \mathfrak{p}) = 1$, $1 \le c \le m-1$. *При этом* $b < c$.

Тогда если r *— четное, то* $\psi_r(w)$ *можно представить в виде многочлена:*

$$\psi_r(w) = C_0^r + C_1^r w + C_2^r w^2 + \ldots + C_{2m-1}^r w^{2m-1},$$

где

$$C_0^r \equiv \frac{r}{2}\beta \pmod{\mathfrak{p}^{2b}}, \qquad C_1^r \equiv 1 + \frac{r}{2}\cdot\frac{r+2}{2}\gamma \pmod{\mathfrak{p}^{2b}},$$

$$C_2^r \equiv -\frac{r}{2}\alpha^{-1}\beta \pmod{\mathfrak{p}^{2b}}, \qquad C_3^r \equiv -\frac{r^2}{4}\alpha^{-1}\gamma \pmod{\mathfrak{p}^{2b}},$$

$$C_k^r \equiv 0 \pmod{\mathfrak{p}^{[k/2]b}}, \quad k \ge 4.$$

Если r *— нечетное, то* $\psi_r(w)$ *можно представить в виде:*

$$\psi_r(w) = C_{-m}^r w^{-m} \ldots + C_{-2}^r w^{-2} + C_{-1}^r w^{-1} + C_0^r + C_1^r w + C_2^r w^2 + \ldots + C_{m-1}^r w^{m-1},$$

где

$$C_{-2}^r \equiv -\frac{r-1}{2}\alpha\beta \pmod{\mathfrak{p}^{2b}}, C_{-1}^r \equiv \alpha\left(1 - \frac{r-1}{2}\cdot\frac{r+1}{2}\gamma\right) \pmod{\mathfrak{p}^{2b}},$$

$$C_0^r \equiv \frac{r+1}{2}\beta \pmod{\mathfrak{p}^{2b}}, \qquad C_1^r \equiv 0 \pmod{\mathfrak{p}^{2b}},$$

$$C_k^r \equiv 0 \pmod{\mathfrak{p}^{kb}} \quad k \ge 2, \; C_{-k}^r \equiv 0 \pmod{\mathfrak{p}^{(k-1)b}} \quad k \ge 3.$$

Доказательство. Рассмотрим r — четное. Согласно лемме (1)

$$\psi_r(w) = \frac{A_0^r + A_1^r w + \ldots + A_r^r w^r + A_{r+1}^r w^{r+1}}{B_0^r + B_1^r w + \ldots + B_r^r w^r},$$

$$A_0^r \equiv \frac{r}{2}\alpha^{r/2}\beta \pmod{\mathfrak{p}^{2b}}, \qquad B_0^r \equiv \alpha^{r/2} \pmod{\mathfrak{p}^{2b}},$$

$$A_1^r \equiv \alpha^{r/2}\left(1 + \frac{r}{2}\cdot\frac{r+2}{2}\gamma\right) \pmod{\mathfrak{p}^{2b}}, \quad B_1^r \equiv \frac{r}{2}\alpha^{(r-2)/2}\beta \pmod{\mathfrak{p}^{2b}},$$

$$B_2^r \equiv \left(\frac{r}{2}\right)^2 \alpha^{(r-2)/2}\gamma \pmod{\mathfrak{p}^{2b}},$$

$$A_{2k}^r \equiv 0 \pmod{\mathfrak{p}^{2kb}} \quad k \ge 1, \qquad B_{2k}^r \equiv 0 \pmod{\mathfrak{p}^{(2k-1)b}} \quad k \ge 2,$$

$$A_{2k+1}^r \equiv 0 \pmod{\mathfrak{p}^{2kb}} \quad k \ge 1, \qquad B_{2k+1}^r \equiv 0 \pmod{\mathfrak{p}^{(2k+1)b}} \quad k \ge 1.$$

Разложим $\psi_r(w)$ в ряд Тейлора по $\pmod{\mathfrak{p}^m}$. Учитывая ограничения на B_i, число слагаемых в разложении будет конечным.

$$\psi_r(w) = \frac{\alpha^{-r/2}(A_0^r + A_1^r w + \ldots + A_{r+1}^r w^{r+1})}{1 + \alpha^{-r/2}(B_0^r - \alpha^{r/2}) + \alpha^{-r/2}B_1^r w + \ldots + \alpha^{-r/2}B_r^r w^r} \equiv$$

$$\equiv \alpha^{-r/2}(A_0^r + A_1^r w + \ldots + A_{r+1}^r w^{w+1}) \times$$

$$\times [1 - (\alpha^{-r/2}(B_0^r - \alpha^{r/2}) + \alpha^{-r/2}B_1^r w + \ldots + \alpha^{-r/2}B_r^r w^r) +$$

$$+ (\alpha^{-r/2}(B_0^r - \alpha^{r/2}) + \alpha^{-r/2}B_1^r w + \ldots + \alpha^{-r/2}B_r^r w^r)^2 -$$

$$- \ldots +$$

$$+ (-1)^{m-1}(\alpha^{-r/2}(B_0^r - \alpha^{r/2}) + \alpha^{-r/2}B_1^r w + \ldots + \alpha^{-r/2}B_r^r w^r)^{m-1}] \equiv$$

$$\equiv \alpha^{-r/2}(A_0^r + A_1^r w + \ldots + A_{r+1}^r w^{w+1})(D_0^r + D_1^r w + \ldots + D_{2m}^r w^{2m}) \pmod{\mathfrak{p}^m}.$$

С учетом того, что в скобках $(\dots)^t$ свободный член делится на $\mathfrak{p}^{2b}$, коэффициент при w делится на $\mathfrak{p}^b$, коэффициенты при w^k делятся на $\mathfrak{p}^{b(k-1)}$, что

$$D_0^r \equiv 1 \pmod{\mathfrak{p}^{2b}}, \qquad D_1^r \equiv -\frac{r}{2}\alpha^{-1}\beta \pmod{\mathfrak{p}^{2b}},$$
$$D_2^r \equiv -\frac{r^2}{4}\alpha^{-1}\gamma \pmod{\mathfrak{p}^{2b}}, D_k^r \equiv 0 \pmod{\mathfrak{p}^{\lceil k/2\rceil b} = \mathfrak{p}^{[(k+1)/2]b}}.$$

Наконец подсчитаем C_i^r.

$$C_0^r = \alpha^{-r/2}A_0^r D_0^r \equiv \frac{r}{2}\beta \pmod{\mathfrak{p}^{2b}},$$
$$C_1^r = \alpha^{-r/2}(A_0^r D_1^r + A_1^r D_0^r) \equiv \alpha^{-r/2}A_1^r D_0^r \equiv 1 + \frac{r}{2}\cdot\frac{r+2}{2}\gamma \pmod{\mathfrak{p}^{2b}},$$
$$C_2^r = \alpha^{-r/2}(A_0^r D_2^r + A_1^r D_1^r + A_2^r D_0^r) \equiv \alpha^{-r/2}A_1^r D_1^r \equiv -\frac{r}{2}\alpha^{-1}\beta \pmod{\mathfrak{p}^{2b}},$$
$$C_3^r \equiv \alpha^{-r/2}A_1^r D_2^r \equiv -\frac{r^2}{4}\alpha^{-1}\gamma \pmod{\mathfrak{p}^{2b}},$$
$$C_k^r \equiv 0 \pmod{\mathfrak{p}^{[k/2]b}} \quad k \geq 4.$$

Аналогично рассматривается случай нечетного r. □

2. Период $\psi_r(w)$.

Представление $\psi_r(w)$, полученное в теореме (1), позволяет получить важные свойства последовательности (2). В частности, позволяет найти период этой последовательности.

Теорема 2. *Пусть $\beta = \mathfrak{p}^b\beta_0$, $(\beta_0, \mathfrak{p}) = 1$, $1 \leq b \leq m-1$, $\gamma = \mathfrak{p}^c\gamma_0$, $(\gamma_0, \mathfrak{p}) = 1$, $1 \leq c \leq m-1$. При этом $b < c$ и $b \geq m/2$. Полагаем, что выполнено неравенство $w^2 \neq \alpha \pmod{\mathfrak{p}}$.*

Тогда период τ последовательности (2) равен

$$\tau = 2\mathfrak{p}^{m-b}, \quad \textit{если} \quad (\mathfrak{p}, \bar{\mathfrak{p}}) = \mathfrak{p}; \qquad \tau = 2N(\mathfrak{p})^{m-b}, \quad \textit{если} \quad (\mathfrak{p}, \bar{\mathfrak{p}}) = 1.$$

Доказательство. Согласно теореме (1)

$$\psi_{2t}(w) = t\beta + (1 + t(t+1)\gamma)w - t\alpha^{-1}\beta w^2 - t^2\alpha^{-1}\gamma w^3 + \mathfrak{p}^{2b}G(w).$$

Учитывая, что $2b \geq m$, запишем

$$\psi_{2t}(w) - \psi_{2s}(w) = (t-s)(\beta + (t+s+1)\gamma w - \alpha^{-1}\beta w^2 - (t+s)\alpha^{-1}\gamma w^3). \qquad (4)$$

Правая скобка в (4) делится строго на $\mathfrak{p}^b$, так как $\beta - \alpha^{-1}\beta w^2 \not\equiv 0 \pmod{\mathfrak{p}}$, а $(t+s+1)\gamma w - (t+s)\alpha^{-1}\gamma w^3$ делится на $\mathfrak{p}^c$, $c > b$.

Рассмотрим случай $(\mathfrak{p}, \bar{\mathfrak{p}}) = 1$. Если $\psi_{2t}(w) \equiv \psi_{2s}(w) \pmod{\mathfrak{p}^m}$, то $\mathfrak{p}^{m-b} | t-s$. Покажем, что $N(\mathfrak{p})^{m-b}$ так же делит $t-s$. Действительно, $\mathfrak{p}|t-s$, $t-s$ — целое рациональное, значит $\bar{\mathfrak{p}}|t-s$. Так как $(\mathfrak{p}, \bar{\mathfrak{p}}) = 1$, то $N(\mathfrak{p})|t-s$. Повторив эту процедуру $m-b$ раз, получим требуемое. Таким образом, если $\psi_{2t}(w) \equiv \psi_{2s}(w) \pmod{\mathfrak{p}^m}$, то $N(\mathfrak{p})^{m-b}|t-s$, а значит, период τ_1 последовательности $\{\psi_{2t}(w)\}$ равен $\tau_1 = N(\mathfrak{p})^{m-b}$.

Легко проверить, что из $\psi_{2t}(w) = \psi_{2s}(w)$ следует $\psi_{2t+1}(w) = \psi_{2s+1}(w)$, если $t - s = \tau_1 = N(\mathfrak{p})^{m-b}$.

$$\frac{\alpha}{\psi_{2t}(w)} + \beta + (2t+1)\gamma w = \frac{\alpha}{\psi_{2s}(w)} + \beta + (2s+1)\gamma w \pmod{\mathfrak{p}^m},$$

$$2(t-s)\gamma w = 0 \pmod{\mathfrak{p}^m}.$$

Тем самым окончательно получаем $\tau = 2\tau_1 = 2N(\mathfrak{p})^{m-b}$.

Аналогично рассматривается случай $(\mathfrak{p}, \bar{\mathfrak{p}}) = \mathfrak{p}$. □

3. Оценка дискрепанции в среднем по w.

Введем в рассмотрение следующую тригонометрическую сумму —

$$\sigma_{k,l}(h) = \sum_{w \in \mathbb{Z}^*_{\mathfrak{p}^m}[i]} \exp\left(\pi i Sp\left(h\frac{\psi_k(w) - \psi_l(w)}{\mathfrak{p}^m}\right)\right),$$

где $h \in \mathbb{Z}_{\mathfrak{p}^m}[i]$ — произвольное.

Будем оценивать $\sigma_{k,l}(h)$ сверху. Для начала нам понадобится несколько вспомогательных лемм.

Лемма 2. *Пусть*

$$F(x) = \ldots + \alpha_{-2}x^{-2} + \alpha_{-1}x^{-1} + \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \ldots$$

$$\alpha_{-2} \not\equiv 0 \pmod{\mathfrak{p}}, \qquad \alpha_0 - \textit{любое}, \qquad \alpha_i \equiv 0 \pmod{\mathfrak{p}} \quad i \neq -2, 0.$$

Тогда

$$S = \sum_{x \in \mathbb{Z}^*_{\mathfrak{p}^m}[i]} \exp\left(\pi i Sp\left(\frac{F(x)}{\mathfrak{p}^m}\right)\right) = 0.$$

Доказательство. Сделаем замену $x = u + \mathfrak{p}^{m-1}v$, $u \in \mathbb{Z}^*_{\mathfrak{p}^{m-1}}[i]$, $v \in \mathbb{Z}_{\mathfrak{p}^m}[i]$. $x^{-1} = u^{-1} - \mathfrak{p}^{m-1}u^{-2}v$. Подставим это в выражение для $F(x)$.

$$\begin{aligned} F(u + \mathfrak{p}^{m-1}v) = \ldots &+ \alpha_{-3}(u^{-1} - \mathfrak{p}^{m-1}u^{-2}v)^3 + \alpha_{-2}(u^{-1} - \mathfrak{p}^{m-1}u^{-2}v)^2 + \\ &+ \alpha_{-1}(u^{-1} - \mathfrak{p}^{m-1}u^{-2}v) + \alpha_0 + \alpha_1(u + \mathfrak{p}^{m-1}v) + \\ &+ \alpha_2(u + \mathfrak{p}^{m-1}v)^2 + \alpha_3(u + \mathfrak{p}^{m-1}v)^3 + \ldots = \\ &= F(u) - 2\alpha_{-2}\mathfrak{p}^{m-1}u^{-3}v, \end{aligned}$$

$$S = \sum_{u \in \mathbb{Z}^*_{\mathfrak{p}^{m-1}}[i]} \exp\left(\pi i Sp\left(\frac{F(u)}{\mathfrak{p}^m}\right)\right) \sum_{v \in \mathbb{Z}_{\mathfrak{p}}[i]} \exp\left(\pi i Sp\left(\frac{-2\alpha_{-2}u^{-3}v}{\mathfrak{p}}\right)\right).$$

Хорошо известно, что сумма по v отлична от нуля только в том случае, когда $-2\alpha_{-2}u^{-3} = 0 \pmod{\mathfrak{p}}$. Но не существует $u \in \mathbb{Z}^*_{\mathfrak{p}^{m-1}}[i]$, чтоб это оказалось верным. Следовательно, сумма по v равна 0 и $S = 0$. □

Последующие леммы используют аналогичную идею для доказательства и мы приведем только их формулировки.

Лемма 3. *Пусть*

$$F(w) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \dots$$

$$\alpha_2 \not\equiv 0 \pmod{\mathfrak{p}}, \qquad \alpha_0 - \textit{любое}, \qquad \alpha_i \equiv 0 \pmod{\mathfrak{p}} \quad i \neq 2, 0.$$

Тогда

$$S = \sum_{x \in \mathbb{Z}^*_{\mathfrak{p}^m}[i]} \exp\left(\pi i Sp\left(\frac{F(x)}{\mathfrak{p}^m}\right)\right) = 0.$$

Лемма 4. *Пусть*

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

$$\alpha_2 \not\equiv 0 \pmod{\mathfrak{p}}, \qquad \alpha_k \equiv 0 \pmod{\mathfrak{p}} \quad k \geq 3.$$

Тогда

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

Лемма 5. *Пусть*

$$F(w) = \dots + \alpha_{-2} w^{-2} + \alpha_{-1} w^{-1} + \alpha_0 + \alpha_1 w + \alpha_2 w^2 + \dots$$

$$\alpha_{-1} \not\equiv 0 \pmod{\mathfrak{p}}, \qquad \alpha_1 \not\equiv 0 \pmod{\mathfrak{p}}, \qquad \alpha_0 - \textit{любое},$$
$$\alpha_i \equiv 0 \pmod{\mathfrak{p}} \quad i \neq -1, 0, 1.$$

Тогда

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

Теперь можно приступить непосредственно к оценке $\sigma_{k,l}(h)$.

Теорема 3. *Пусть* $\beta = \mathfrak{p}^b \beta_0$, $(\beta_0, \mathfrak{p}) = 1$, $1 \leq b \leq m-1$, $\gamma = \mathfrak{p}^c \gamma_0$, $(\gamma_0, \mathfrak{p}) = 1$, $1 \leq c \leq m-1$. *При этом* $b < c$ *и* $b > m/2$. *Требуем, чтоб выполнялось неравенство* $w^2 \not\equiv \alpha \pmod{\mathfrak{p}}$. *Пусть* $h = h_0 \mathfrak{p}^d, (h_0, \mathfrak{p}) = 1, k - l = t_0 \mathfrak{p}^t, (t_0, \mathfrak{p}) = 1$.

Тогда

$$\sigma_{k,l}(h) \leq \begin{cases} 2N(\mathfrak{p})^{(m+d)/2}, & m - d - b - t > 0 \\ N(\mathfrak{p})^m, & m - d - b - t \leq 0. \end{cases}$$

Доказательство. Для начала будем считать что k, l — оба четные. По теореме (1) имеем

$$\psi_k(w) - \psi_l(w) = \frac{k-l}{2}\left(\beta + \frac{k+l+2}{2}\gamma w - \alpha^{-1}\beta w^2 - \frac{k+l}{2}\alpha^{-1}\gamma w^3\right) + \mathfrak{p}^{2b} G_1(w).$$

Заметим, что $(k-l)/2 = (t_0/2)\mathfrak{p}^t$, $(t_0/2, \mathfrak{p}) = 1$. Подставим выражение для $\psi_k(w) - \psi_l(w)$ в $\sigma_{k,l}(h)$.

$$\sigma_{k,l}(h) = N(\mathfrak{p})^{d+b+t} \sum_{w \in \mathbb{Z}^*_{\mathfrak{p}^{m-b-t-d}}[i]} \exp\left(\pi i Sp\left(h_0 \times \right.\right.$$
$$\left.\left. \times \frac{\frac{t_0}{2}(b_0 + \frac{k+l+2}{2} c_0 \mathfrak{p}^{c-b} w - \frac{1}{2}\alpha^{-1} b_0 w^2 - \frac{k+l}{4}\alpha^{-1} c_0 \mathfrak{p}^{c-b} w^3) + \mathfrak{p}^{b-t} G_1(w)}{\mathfrak{p}^{m-b-t-d}}\right)\right).$$

По теореме (2), $t \le m-b$, следовательно, $b - t \ge 2b - m > 0$. Значит можем применить лемму (3) и при условии $m - d - b - t > 0$ получим $\sigma_{k,l}(h) = 0$. Что завершает доказательство теоремы для этого случая.

Теперь будем считать, что k, l — оба нечетные. Пользуемся теоремой (1)

$$\psi_k(w) - \psi_l(w) = \frac{k-l}{2}\left(-\alpha\beta w^{-2} + \frac{k+l}{2}\alpha\gamma w^{-1} + \beta\right) + \mathfrak{p}^{2b} G_2(w).$$

Учтем, что $(k-l)/2 = (t_0/2)\mathfrak{p}^t$, $(t_0/2, \mathfrak{p}) = 1$. Подставим выражение для $\psi_k(w) - \psi_l(w)$ в $\sigma_{k,l}(h)$.

$$\sigma_{k,l}(h) = N(\mathfrak{p})^{d+b+t} \times$$
$$\times \sum_{w \in \mathbb{Z}^*_{\mathfrak{p}^{m-b-t-d}}[i]} \exp\left(\pi i Sp\left(h_0 \frac{\frac{t_0}{2}(-\alpha b_0 w^{-2} + \frac{k-l}{2}\alpha c_0 \mathfrak{p}^{c-b} w^{-1} + b_0) + \mathfrak{p}^{b-t} G_2(w)}{\mathfrak{p}^{m-b-t-d}}\right)\right).$$

Воспользовавшись леммой (2), получим $\sigma_{k,l}(h) = 0$ при условии $m-d-b-t > 0$.

Наконец, рассмотрим случай, когда k, l — разной четности. Так как знак аргумента на модуль суммы не влияет, мы можем считать k — четным, l — нечетным.

$$\psi_k(w) - \psi_l(w) = \frac{k}{2}\beta + \left(1 + \frac{k}{2}\cdot\frac{k+2}{2}\gamma\right) w - \frac{k}{2}\alpha^{-1}\beta w^2 - \frac{k^2}{4}\alpha^{-1}\gamma w^3 +$$
$$+ \frac{l-1}{2}\alpha\beta w^{-2} - \alpha\left(1 - \frac{l-1}{2}\cdot\frac{l+1}{2}\gamma\right) w^{-1} - \frac{l+1}{2}\beta + \mathfrak{p}^{2b} G_3(w),$$

$$\sigma_{k,l}(h) = N(\mathfrak{p})^d \sum_{w \in \mathbb{Z}^*_{\mathfrak{p}^{m-d}}[i]} \exp\left(\pi i Sp\left(h_0 \frac{\psi_k(w) - \psi_l(w)}{\mathfrak{p}^{m-d}}\right)\right).$$

Если $m - d > 0$, то применяя лемму (5), получим

$$|\sigma_{k,l}(h)| \le 2N(\mathfrak{p})^d N(\mathfrak{p})^{(m-d)/2} = 2N(\mathfrak{p})^{(m+d)/2}.$$

□

Определим $S_M(h, w)$ для произвольного целого h и $1 \le M \le \tau$.

$$S_M(h, w) = \sum_{k=0}^{M-1} \exp\left(\pi i Sp\left(\frac{h\psi_k(w)}{\mathfrak{p}^m}\right)\right).$$

Теорема 4. *Пусть* $\beta = \mathfrak{p}^b\beta_0$, $(\beta_0, \mathfrak{p}) = 1$, $1 \le b \le m-1$, $\gamma = \mathfrak{p}^c\gamma_0$, $(\gamma_0, \mathfrak{p}) = 1$, $1 \le c \le m-1$. *При этом* $b < c$ *и* $b > m/2$. *Требуем, чтоб выполнялось неравенство* $w^2 \not\equiv \alpha \pmod{\mathfrak{p}}$. *Пусть* $h = h_0\mathfrak{p}^d, (h_0, \mathfrak{p}) = 1$.

Тогда почти для всех $w \in \mathbb{Z}^*_{\mathfrak{p}^m}$ *верна оценка*

$$|S_M(h,w)| \le 2.7MN(\mathfrak{p})^{-\frac{m-d-b}{4}}.$$

Доказательство. Введем в рассмотрение сумму

$$\overline{S}_M(h) = \frac{1}{|\mathbb{Z}^*_{\mathfrak{p}^m}|}\sum_{w\in\mathbb{Z}^*_{\mathfrak{p}^m}} S_M(h,w).$$

Применим неравенство Коши–Шварца.

$$|\overline{S}_M(h)|^2 \le \frac{1}{|\mathbb{Z}^*_{\mathfrak{p}^m}|}\sum_{w\in\mathbb{Z}^*_{\mathfrak{p}^m}} |S_M(h,w)|^2 =$$

$$= \frac{1}{|\mathbb{Z}^*_{\mathfrak{p}^m}|}\sum_{w\in\mathbb{Z}^*_{\mathfrak{p}^m}}\sum_{k,l=0}^{M-1} \exp\left(\pi i Sp\left(\frac{h(\psi_k(w)-\psi_l(w))}{\mathfrak{p}^m}\right)\right) =$$

$$= \frac{1}{|\mathbb{Z}^*_{\mathfrak{p}^m}|}\sum_{k,l=0}^{M-1}|\sigma_{k,l}(w)| \le \frac{1}{|\mathbb{Z}^*_{\mathfrak{p}^m}|}\sum_{t=0}^{m-b}\sum_{\substack{k,l=0\\ k\equiv l \pmod{\mathfrak{p}^t}}}^{M-1}|\sigma_{k,l}(w)|.$$

Пользуемся теоремой (3).

$$|\overline{S}_M(h)|^2 \le \frac{1}{|\mathbb{Z}^*_{\mathfrak{p}^m}|}\left(\sum_{t=0}^{m-d-b-1} 2N(\mathfrak{p})^{\frac{m+d}{2}}\sum_{\substack{k,l=0\\ k\equiv l \pmod{\mathfrak{p}^t}}}^{M-1} 1 + \sum_{t=m-d-b}^{m-b} N(\mathfrak{p})^m \sum_{\substack{k,l=0\\ k\equiv l \pmod{\mathfrak{p}^t}}}^{M-1} 1\right).$$

Дадим оценку следующей сумме:

$$\sum_{\substack{k,l=0\\ k\equiv l \pmod{\mathfrak{p}^t}}}^{M-1} 1 \le \sum_{\substack{k,l=0\\ N(\mathfrak{p})^t|(k-l)^2}}^{M-1} 1 \le \sum_{\substack{k,l=0\\ N(\mathfrak{p})^{\lceil t/2\rceil}|(k-l)}}^{M-1} 1 \le \sum_{\substack{k,l=0\\ k\equiv l \pmod{N(\mathfrak{p})^{\lceil t/2\rceil}}}}^{M-1} 1 \le \frac{M^2}{N(\mathfrak{p})^{t/2}}.$$

Продолжим оценку $|\overline{S}_M(h)|^2$:

$$|\overline{S}_M(h)|^2 \le \frac{1}{|\mathbb{Z}^*_{\mathfrak{p}^m}|}\left(\sum_{t=0}^{m-d-b-1} 2N(\mathfrak{p})^{\frac{m+d}{2}}\frac{M^2}{N(\mathfrak{p})^{t/2}} + \sum_{t=m-d-b}^{m-b} N(\mathfrak{p})^m\frac{M^2}{N(\mathfrak{p})^{t/2}}\right) \le$$

$$\le \frac{M^2}{|\mathbb{Z}^*_{\mathfrak{p}^m}|}\left(2N(\mathfrak{p})^{\frac{m+d}{2}}\frac{1}{1-N(\mathfrak{p})^{-1/2}} + N(\mathfrak{p})^{d+b}\frac{1}{1-N(\mathfrak{p})^{-1/2}}\right).$$

Учтем, что $|\mathbb{Z}^*_{\mathfrak{p}^m}| = N(\mathfrak{p})^m\left(1-\frac{1}{N(\mathfrak{p})}\right) \ge \frac{2}{3}N(\mathfrak{p})^m$,

$$|\overline{S}_M(h)|^2 \le 1.5\frac{M^2}{N(\mathfrak{p})^m}\left(4.8N(\mathfrak{p})^{\frac{m+d}{2}} + 2.4N(\mathfrak{p})^{d+b}\right) \le 7.2M^2N(\mathfrak{p})^{-\frac{m-d-b}{2}}.$$

Значит, $|\overline{S}_M(h)| \le 2.7MN(\mathfrak{p})^{-\frac{m-d-b}{4}}$. Что завершает доказательство теоремы. □

Теперь у нас есть все необходимые результаты для оценки дискрепанции в среднем по $w \in \mathbb{Z}^*_{\mathfrak{p}^m}$.

Теорема 5. *Пусть* $\beta = \mathfrak{p}^b\beta_0$, $(\beta_0, \mathfrak{p}) = 1$, $1 \le b \le m-1$, $\gamma = \mathfrak{p}^c\gamma_0$, $(\gamma_0, \mathfrak{p}) = 1$, $1 \le c \le m-1$. *При этом* $b < c$ *и* $b > m/2$. *Требуем, чтоб выполнялось неравенство* $w^2 \not\equiv \alpha \pmod{\mathfrak{p}}$.

Тогда почти для всех $w \in \mathbb{Z}^*_{\mathfrak{p}^m}$ *дискрепанция последовательности (3) оценивается как*

$$D_M(w) < 28.5N(\mathfrak{p})^{-(m-b)/4} \ln N(\mathfrak{p})^{m-b}.$$

Доказательство. Будем пользоваться хорошо известной в литературе оценкой ([5])

$$D_M(w) \le \frac{1}{H+1} + \frac{2}{M}\sum_{h=1}^{H}\left(\frac{1}{\pi h} + \frac{1}{H+1}\right)|S_M(h,w)|. \tag{5}$$

Оценим

$$\sum_{\substack{h=1\\ \mathfrak{p}^d|h}}^{H}\frac{1}{h} \le \sum_{\substack{h=1\\ N(\mathfrak{p})^d|h^2}}^{H}\frac{1}{h} \le \sum_{\substack{h=1\\ N(\mathfrak{p})^{\lceil d/2\rceil}|h}}^{H}\frac{1}{h} \le \frac{1}{N(\mathfrak{p})^{d/2}}\left(1 + \ln\frac{H}{N(\mathfrak{p})^{d/2}}\right) \le \frac{1}{N(\mathfrak{p})^{d/2}}\left(1+\ln H\right).$$

Из теоремы (4) следует, что почти для всех w

$$\begin{aligned}\sum_{h=1}^{H}\frac{1}{h}|S_M(h,w)| &< 2.7MN(\mathfrak{p})^{-(m-b)/4}\sum_{d=0}^{\infty}N(\mathfrak{p})^{d/4}\sum_{\substack{h=1\\ \mathfrak{p}^d|h}}^{H}\frac{1}{h} = \\ &= 2.7MN(\mathfrak{p})^{-(m-b)/4}(1+\ln H)\frac{1}{1-N(\mathfrak{p})^{-1/4}} < \\ &< 11.4MN(\mathfrak{p})^{-(m-b)/4}(1+\ln H).\end{aligned} \tag{6}$$

Аналогично получим оценку для суммы

$$\sum_{h=1}^{H}|S_M(h,w)| < 11.4MN(\mathfrak{p})^{-(m-b)/4}H. \tag{7}$$

Подставляем оценки (6) и (7) в (5).

$$D_M(w) < \frac{1}{H+1} + 22.8N(\mathfrak{p})^{-(m-b)/4}\left(\frac{1}{\pi}(1+\ln H)+1\right).$$

Выберем $H = \lfloor N(\mathfrak{p})^{(m-b)/4}\rfloor$. Тогда $H+1 \ge N(\mathfrak{p})^{(m-b)/4}$ и $(H+1)^{-1} \le N(\mathfrak{p})^{-(m-b)/4}$.

$$\begin{aligned}D_M(w) &< N(\mathfrak{p})^{-(m-b)/4} + 22.8N(\mathfrak{p})^{-(m-b)/4}\left(\frac{1}{\pi}\left(1+\ln N(\mathfrak{p})^{(m-b)/4}\right)+1\right) \le \\ &\le N(\mathfrak{p})^{-(m-b)/4}\left(31.1 + \frac{1}{4\pi}\ln N(\mathfrak{p})^{m-b}\right) \le \\ &\le 28.5N(\mathfrak{p})^{-(m-b)/4}\ln N(\mathfrak{p})^{m-b}.\end{aligned}$$

□

4. Оценка дискрепанции для индивидуального w, $(w,\mathfrak{p})=1$.

Получим оценку полной тригонометрической суммы $S_\tau(h,w)$.

Теорема 6. *Пусть $\beta=\mathfrak{p}^b\beta_0$, $(\beta_0,\mathfrak{p})=1$, $1\le b\le m-1$, $\gamma=\mathfrak{p}^c\gamma_0$, $(\gamma_0,\mathfrak{p})=1$, $1\le c\le m-1$. При этом $b<c$ и $b\ge m/2$. Пусть $h=h_0\mathfrak{p}^d$, $(h_0,\mathfrak{p})=1$. Требуем, чтоб для $(\mathfrak{p},\bar{\mathfrak{p}})=\mathfrak{p}$ выполнялись неравенства*

$$\begin{aligned} Re(\beta_0-\alpha^{-1}\beta_0w^2)&\not\equiv 0 \pmod{\mathfrak{p}},\\ Re(\beta_0-\alpha\beta_0w^{-2})&\not\equiv 0 \pmod{\mathfrak{p}}. \end{aligned} \tag{8}$$

Для $(\mathfrak{p},\bar{\mathfrak{p}})=1$.

$$\begin{aligned} Re(\bar{\mathfrak{p}}^{m-b}\beta_0-\bar{\mathfrak{p}}^{m-b}\alpha^{-1}\beta_0w^2)&\not\equiv 0 \pmod{N(\mathfrak{p})},\\ Re(\bar{\mathfrak{p}}^{m-b}\beta_0-\bar{\mathfrak{p}}^{m-b}\alpha\beta_0w^{-2})&\not\equiv 0 \pmod{N(\mathfrak{p})}. \end{aligned} \tag{9}$$

Тогда

$$|S_\tau(h,w)|\le\begin{cases}0, & m-b-d>0,\\ \tau, & m-b-d\le 0.\end{cases}$$

Замечание 1. *Условия (8) и (9) являются уточнением условия $w^2\not\equiv\alpha \pmod{\mathfrak{p}}$.*

Доказательство.

$$|S_\tau(h,w)|\le\left|\sum_{t=0}^{\tau/2}\exp\left(\pi iSp\left(\frac{h\psi_{2t}(w)}{\mathfrak{p}^m}\right)\right)\right|+\left|\sum_{t=0}^{\tau/2}\exp\left(\pi iSp\left(\frac{h\psi_{2t+1}(w)}{\mathfrak{p}^m}\right)\right)\right|.$$

По теореме (1)

$$\begin{aligned}\psi_{2t}(w)&=w+(\beta+\gamma w-\alpha^{-1}\beta w^2)t+(\gamma w-\alpha^{-1}\gamma w^3)t^2+\mathfrak{p}^{2b}G_1(w),\\ \psi_{2t+1}(w)&=\beta+\alpha w^{-1}+(\beta-\alpha\gamma w^{-1}-\alpha\beta w^{-2})t-\alpha\gamma w^{-1}t^2+\mathfrak{p}^{2b}G_2(w).\end{aligned}$$

Рассмотрим случай $(\mathfrak{p},\bar{\mathfrak{p}})=\mathfrak{p}$. Тогда по теореме (2) $\tau=2\mathfrak{p}^{m-b}$

$$\begin{aligned}|S_\tau(h,w)|\le\mathfrak{p}^d&\left|\sum_{t=0}^{\mathfrak{p}^{m-b-d}}\exp\Bigg(2\pi ih_0\times\right.\\ &\left.\times\frac{Re(\beta_0+\gamma_0\mathfrak{p}^{c-b}w-\alpha^{-1}\beta_0w^2)t+Re(\gamma_0\mathfrak{p}^{c-b}w-\alpha^{-1}\gamma_0\mathfrak{p}^{c-b}w^3)t^2}{\mathfrak{p}^{m-b-d}}\Bigg)\right|+\\ +\mathfrak{p}^d&\left|\sum_{t=0}^{\mathfrak{p}^{m-b-d}}\exp\left(2\pi ih_0\frac{Re(\beta_0-\alpha\gamma_0\mathfrak{p}^{c-b}w^{-1}-\alpha\beta_0w^{-2})t-Re(\alpha\gamma_0\mathfrak{p}^{c-b}w^{-1})t^2}{\mathfrak{p}^{m-b-d}}\right)\right|.\end{aligned}$$

Мы получили 2 обычных суммы Гаусса. В каждой сумме коэффициент при t^2 делится по крайней мере на $\mathfrak{p}^{c-b}$, а коэффициент при t не делится на $\mathfrak{p}^{c-b}$. Известно, что в этом случае сумма Гаусса равна 0. Значит,

$$|S_\tau(h,w)|\le\begin{cases}0, & m-b-d>0,\\ 2\mathfrak{p}^{m-b}, & m-b-d\le 0.\end{cases}$$

Случай $(\mathfrak{p},\bar{\mathfrak{p}})=1$ рассматривается аналогично. □

Теперь получим оценку неполной тригонометрической суммы через полную.

Теорема 7. *Пусть* $\beta = \mathfrak{p}^b\beta_0$, $(\beta_0, \mathfrak{p}) = 1$, $1 \le b \le m-1$, $\gamma = \mathfrak{p}^c\gamma_0$, $(\gamma_0, \mathfrak{p}) = 1$, $1 \le c \le m-1$. *При этом* $b < c$ *и* $b \ge m/2$. *Пусть* $h = h_0\mathfrak{p}^d$, $(h_0, \mathfrak{p}) = 1$.

Если $(\mathfrak{p}, \bar{\mathfrak{p}}) = \mathfrak{p}$ *и выполнены условия*

$$\begin{aligned} Re(\beta_0 - \alpha^{-1}\beta_0 w^2) &\not\equiv 0 \pmod{\mathfrak{p}},\\ Re(\beta_0 - \alpha\beta_0 w^{-2}) &\not\equiv 0 \pmod{\mathfrak{p}},\\ Re(\gamma_0 w - \alpha^{-1}\gamma_0 w^3) &\not\equiv 0 \pmod{\mathfrak{p}},\\ Re(\gamma_0\alpha w^{-1}) &\not\equiv 0 \pmod{\mathfrak{p}}, \end{aligned}$$

то справедлива оценка

$$|S_M(h,w)| \le \begin{cases} 2\mathfrak{p}^{\frac{m-d+c-2b}{2}}\ln\tau, & m-b-d>0,\\ M, & m-b-d\le 0. \end{cases}$$

Если $(\mathfrak{p}, \bar{\mathfrak{p}}) = 1$ *и выполнены условия*

$$\begin{aligned} Re(\bar{\mathfrak{p}}^{m-b}(\beta_0 - \alpha^{-1}\beta_0 w^2)) &\not\equiv 0 \pmod{N(\mathfrak{p})},\\ Re(\bar{\mathfrak{p}}^{m-b}(\beta_0 - \alpha\beta_0 w^{-2})) &\not\equiv 0 \pmod{N(\mathfrak{p})},\\ Re(\bar{\mathfrak{p}}^{m-c}(\gamma_0 w - \alpha^{-1}\gamma_0 w^3)) &\not\equiv 0 \pmod{N(\mathfrak{p})},\\ Re(\bar{\mathfrak{p}}^{m-c}\gamma_0\alpha w^{-1}) &\not\equiv 0 \pmod{N(\mathfrak{p})}, \end{aligned}$$

то справедлива оценка

$$|S_M(h,w)| \le \begin{cases} 2N(\mathfrak{p})^{\frac{m-d+c-2b}{2}}\ln\tau, & m-b-d>0,\\ M, & m-b-d\le 0. \end{cases}$$

Доказательство. Воспользуемся тем, что при целых $0 \le k, l < \tau$

$$\frac{1}{\tau}\sum_{x=0}^{\tau-1}\exp\left(2\pi i\frac{(k-l)x}{\tau}\right) = \begin{cases} 0, & k\ne l,\\ 1, & k = l. \end{cases}$$

Тогда $|S_M(h,w)|$ можно представить как

$$\begin{aligned} |S_M(h,w)| &= \left|\sum_{l=0}^{M-1}\sum_{k=0}^{\tau-1}\exp\left(\pi i Sp\left(\frac{h\psi_k(w)}{\mathfrak{p}^m}\right)\right)\frac{1}{\tau}\sum_{x=0}^{\tau-1}\exp\left(2\pi i\frac{(k-l)x}{\tau}\right)\right| =\\ &= \frac{1}{\tau}\left|\sum_{x=0}^{\tau-1}\sum_{k=0}^{\tau-1}\sum_{l=0}^{M-1}\exp\left(\pi i Sp\left(\frac{h\psi_k(w)}{\mathfrak{p}^m}\right)\right)\exp\left(2\pi i\frac{(k-l)x}{\tau}\right)\right|. \end{aligned}$$

Отделим слагаемое $x = 0$.

$$\begin{aligned} |S_M(h,w)| &\le \frac{M}{\tau}\left|\sum_{k=0}^{\tau-1}\exp\left(\pi i Sp\frac{h\psi_k(w)}{\mathfrak{p}^m}\right)\right| +\\ &+ \left|\sum_{x=1}^{\tau-1}\sum_{k=0}^{\tau-1}\exp\left(\pi i Sp\left(\frac{h\psi_k(w)}{\mathfrak{p}^m}\right)\right)\exp\left(2\pi i\frac{kx}{\tau}\right)\frac{1}{\tau}\sum_{l=0}^{M-1}\exp\left(2\pi i\frac{-xl}{\tau}\right)\right| \le\\ &\le \frac{M}{\tau}|S_\tau(h,w)| + \sum_{x=1}^{\tau-1}\frac{1}{2\min(x,\tau-x)}\left|\sum_{k=0}^{\tau-1}\exp\left(\pi i\left(Sp\frac{h\psi_k(w)}{\mathfrak{p}^m} + 2\frac{kx}{\tau}\right)\right)\right|. \end{aligned}$$

Рассмотрим отдельно

$$\left|\sum_{k=0}^{\tau-1}\exp\left(\pi i\left(Sp\frac{h\psi_k(w)}{\mathfrak{p}^m}+2\frac{kx}{\tau}\right)\right)\right|\le$$
$$\le\left|\sum_{t=0}^{\tau/2-1}\exp\left(\pi i\left(Sp\frac{h\psi_{2t}(w)}{\mathfrak{p}^m}+\frac{4tx}{\tau}\right)\right)\right|+\left|\sum_{t=0}^{\tau/2-1}\exp\left(\pi i\left(Sp\frac{h\psi_{2t+1}(w)}{\mathfrak{p}^m}+\frac{4tx}{\tau}\right)\right)\right|.$$

Пусть $(\mathfrak{p},\bar{\mathfrak{p}})=\mathfrak{p}$. Тогда используя теоремы (1) и (2), имеем

$$|S_1|=\left|\sum_{t=0}^{\tau/2-1}\exp\left(\pi i\left(Sp\frac{h\psi_{2t}(w)}{\mathfrak{p}^m}+\frac{4tx}{\tau}\right)\right)\right|=\left|\sum_{t=0}^{\mathfrak{p}^{m-b}-1}\exp\Bigg(2\pi i\times\right.$$
$$\left.\times\frac{(hRe(\beta_0+\mathfrak{p}^{c-b}\gamma_0 w-\alpha^{-1}\beta_0 w^2)+x)t+h\mathfrak{p}^{c-b}Re(\gamma_0 w-\alpha^{-1}\gamma_0 w^3)t^2}{\mathfrak{p}^{m-b}}\Bigg)\right|.$$

Коэффициент при t^2 делится строго на $\mathfrak{p}^{d+c-b}$. Следовательно, чтоб сумма Гаусса S_1 допускала ненулевую оценку, необходимо, чтобы

$$hRe(\beta_0+\gamma_0\mathfrak{p}^{c-b}w-\alpha^{-1}\beta_0 w^2)+x\equiv 0\pmod{\mathfrak{p}^{d+c-b}}$$
$$x\equiv 0\pmod{\mathfrak{p}^d}.$$

В результате при $m-b-d>0$ S_1 можно оценить как $|S_1|\le\mathfrak{p}^{\frac{(m-b)+(d+c-b)}{2}}=$ $=\mathfrak{p}^{\frac{m+d+c-2b}{2}}$. К точно такому же результату приводит рассмотрение суммы

$$S_2=\sum_{t=0}^{\tau/2-1}\exp\left(Sp\frac{h\psi_{2t+1}(w)}{\mathfrak{p}^m}+\frac{4tx}{\tau}\right).$$

При $x\equiv 0\pmod{\mathfrak{p}^d}$, $m-b-d>0$ получается оценка $|S_2|\le\mathfrak{p}^{\frac{m+d+c-2b}{2}}$. Если $x\not\equiv 0\pmod{\mathfrak{p}^d}$, то $|S_2|=0$. Подставим эти результаты в оценку $|S_M(h,w)|$.

$$|S_M(h,w)|\le\frac{M}{\tau}|S_\tau(h,w)|+\sum_{\substack{x=0\\(\mathrm{mod}\ \mathfrak{p}^d)}}^{\tau-1}\sum_{x=1}\frac{1}{2\min(x,\tau-x)}2\mathfrak{p}^{\frac{m+d+c-2b}{2}}\le$$
$$\le\frac{M}{\tau}|S_\tau(h,w)|+2\mathfrak{p}^{\frac{m+d+c-2b}{2}}\sum_{x=1}^{\tau}\frac{1}{\mathfrak{p}^d x}\le 2\mathfrak{p}^{\frac{m-d+c-2b}{2}}\ln\tau.$$

Аналогично рассматривая случай $(\mathfrak{p},\bar{\mathfrak{p}})=1$, придем к оценке $|S_M(h,w)|\le$ $\le 2N(\mathfrak{p})^{\frac{m-d+c-2b}{2}}\ln\tau$.

□

Теорема 8. *Пусть* $\beta=\mathfrak{p}^b\beta_0$, $(\beta_0,\mathfrak{p})=1$, $1\le b\le m-1$, $\gamma=\mathfrak{p}^c\gamma_0$, $(\gamma_0,\mathfrak{p})=1$, $1\le c\le m-1$. *При этом* $b<c$ *и* $b\ge m/2$. *Пусть* $h=h_0\mathfrak{p}^d$, $(h_0,\mathfrak{p})=1$.

Полагаем, что выполнены условия на α, β, γ, w *из предыдущей теоремы. Тогда если* $(\mathfrak{p},\bar{\mathfrak{p}})=\mathfrak{p}$, *справедлива оценка*

$$D_M(w)\le M^{-1}\mathfrak{p}^{(c-b)/2}\tau^{1/2}\ln\tau\,(1.6\ln M+6.9).$$

Если $(\mathfrak{p}, \bar{\mathfrak{p}}) = 1$, *то*

$$D_M(w) \le M^{-1} N(\mathfrak{p})^{(c-b)/2} \tau^{1/2} \ln \tau \, (1.6 \ln M + 6.9) \, .$$

Доказательство.
Будем пользоваться неравенством Эрдеса–Турана:

$$D_M(w) \le \frac{1}{H+1} + \frac{2}{M} \sum_{h=1}^{H} \left(\frac{1}{\pi h} + \frac{1}{H+1} \right) |S_M(h, w)|. \tag{10}$$

Рассмотрим случай $(\mathfrak{p}, \bar{\mathfrak{p}}) = \mathfrak{p}$. Оценим следующие суммы с помощью теоремы (7).

$$\sum_{h=1}^{H} \frac{1}{h} |S_M(h, w)| < 2\mathfrak{p}^{\frac{m+c-2b}{2}} \ln \tau \sum_{d=0}^{\infty} \mathfrak{p}^{d/2} \sum_{\substack{h=1 \\ \mathfrak{p}^d | h}}^{H} \frac{1}{h} < 4.8\mathfrak{p}^{\frac{m+c-2b}{2}} \ln \tau (1 + \ln H)$$

$$\sum_{h=1}^{H} |S_M(h, w)| < 4.8\mathfrak{p}^{\frac{m+c-2b}{2}} \ln \tau H.$$

Подставляем полученные оценки в (10).

$$D_M(w) \le \frac{1}{H+1} + 9.6 M^{-1} \mathfrak{p}^{\frac{m+c-2b}{2}} \ln \tau \left(\frac{1}{\pi} (1 + \ln H) + 1 \right).$$

Берем H равным $H = \lfloor M \mathfrak{p}^{-\frac{m+c-2b}{2}} \ln^{-1} \tau \rfloor$.

$$D_M(w) \le M^{-1} \mathfrak{p}^{\frac{m+c-2b}{2}} \ln \tau \left(\frac{9.6}{\pi} \left(1 + \ln \left(M \mathfrak{p}^{-\frac{m+c-2b}{2}} \ln^{-1} \tau \right) \right) + 10.6 \right) \le$$
$$\le M^{-1} \mathfrak{p}^{(c-b)/2} \tau^{1/2} \ln \tau \, (1.6 \ln M + 6.9) \, .$$

Абсолютно аналогично получаем результат для случая $(\mathfrak{p}, \bar{\mathfrak{p}}) = 1$.

$$D_M(w) \le M^{-1} N(\mathfrak{p})^{(c-b)/2} \tau^{1/2} \ln \tau \, (1.6 \ln M + 6.9) \, .$$

□

Заключение. Полученный период последовательности (2) показывает, что добавление переменного сдвига в инверсный конгруэнтный генератор не ухудшает его периода. Полученные оценки дискрепанции не являются тривиальными и указывают на равномерность распределения чисел последовательности (3). В последующих работах мы планируем избавиться от ограничения $b \ge m/2$ и получить аналогичные результаты.

1. **H. Niederreiter.** Random number generation and quasi-Monte Carlo methods [text] / H. Niederreiter. – SIAM, Philadelphia, 1992.

2. **H. Niederreiter.** On the distribution of inversive congruential pseudorandom numbers in parts of the period [text] / H. Niederreiter, I. E. Shparlinski // Math. Comput. 70(236). – 2001. – P. 1569–1574.

3. **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.

4. **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.

5. **J. D. Vaaler.** Some extremal functions in Fourier analysis [text] / J. D. Vaaler // Bull. Amer. Math. Soc. (N.S.) 12. – 1985. – P. 183–216.

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. **H. Niederreiter.** The serial test for congruential pseudorandom numbers generated by inversions [text] / H. Niederreiter // Math. Comp. 52. – 1989. – P. 135–144.

8. **H. Niederreiter.** New developments in uniform pseudorandom number and vector generation [text] / H. Niederreiter // Lect. Notes in Statistics 106. – Springer-Verlag, Berlin, 106. – 1995. – P. 87–120.

9. **J. Eichenauer.** A nonlinear congruential pseudorandom number generator with power of two modules [text] / J. Eichenauer, J. Lehn, A. Topuzoglu // Math. Comp. 51. – 1988. – P. 757–759.

10. **J. Eichenauer-Herrmann.** On the period of congruential pseudorandom number sequences generated by inversions [text] / J. Eichenauer-Herrmann, A. Topuzoglu // J. Comput. Appl. Math. 31. – 1990. – P. 87-96.