С.А. Задорожный (Одесский национальный университет им. И.И. Мечникова, Одесса, Украина)

Инверсный конгруентальный генератор над $\mathbb{Z}[i]$.

Обозначим через $\mathbb{Z}[i]$ кольцо целых Гауссовых чисел $\mathbb{Z}[i] = \{a+bi \mid a,b \in \mathbb{Z},\ i^2 = -1\}$. Пусть p - простое Гауссово число, а $N(p)$ - его норма. Пусть $\alpha, \beta \in \mathbb{Z}[i]$ такие, что $(\alpha, p) = 1$, $\beta = 0 \pmod p$. Определим следующее рекурсивное соотношение

$$w_{n+1} = \alpha w_n^{-1} + \beta \pmod{p^m} \tag{1}$$

где $m \in \mathbb{N}$, $w_0 \in \mathbb{Z}[i]$, $(w_0, p) = 1$ - фиксированные числа, w^{-1} обозначает мультипликативнообратное к w по модулю p^m.

Последовательность $\{w_n\}$, генерируемая генератором (1), называется последовательностью инверсных конгруентальных псевдослучайных Гауссовых чисел. Это определение является аналогом последовательности псевдослучайных чисел над $\mathbb{Z}$, которая впервые была изучена Нидеррайтером и Шпарлинским в [1].

В своей работе мы получаем оценку специальной тригонометрической суммы

$$\sigma_r(p^m) = \sum_{\substack{w_0 \in \mathbb{Z}_{p^m} \\ (w_0,p)=1}} e^{\pi i Sp(\frac{w_r - w_0}{p^m})}$$

где $Sp(z) = 2Re\ z$, $z \in \mathbb{C}$.

Теорема 1 *Для $m \geq 2$ и r - нечетного справедлива оценка:*

$$\sigma_r(p^m) << N(p)^{\frac{m}{2}}$$

Теорема 2 *Пусть $\beta = \beta_0 p^b$, $(\beta_0, p) = 1$ и r - четное. Тогда справедливо неравенство:*

$$\sigma_r(p^m) \leq DN(p)^{\frac{m+b+\varepsilon_b}{2}}, \quad \varepsilon_b = \begin{cases} 0 & if \quad m = b \pmod 2 \\ 1 & if \quad m \neq b \pmod 2 \end{cases}$$

Здесь через D обозначено число решений сравнения

$$2\beta_0 u^3 = (-1)^{r/2} \pmod{p^{m_1}}, \qquad m_1 = [(m-b)/2]$$

Полученные теоремы об оценки тригонометрической суммы $\sigma_r(p^m)$ позволяют получить нетривиальную оценку дискрепнции последовательности $\left\{\frac{w_n}{N(p)^m}\right\}$ в квадрате $[-1,1]^2$.

[1] Niederreiter, H. and Shparlinski, I.E., Exponential sums and the distribution of inversive congruential pseudorandom numbers with prime-power modulus. Acta Arith. v92 i1. 89-98.