ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 28 МАТЕМАТИКИ Выпуск 1
2021

**В. А. Едемский**, **О. О. Чуркин**, **С. А. Кольцова** (Великий Новгород, НовГУ). **О симметричной $p$-адической сложности циклотомических и обобщенных циклотомических последовательностей.**

УДК 519.7

*Резюме*: Исследуется $p$-адическая сложность ряда циклотомических последовательностей малых порядков. Показано, что эти последовательности имеют высокую симметричную $p$-адическую сложность. Отдельные результаты получены для обобщенных циклотомических последовательностей.

*Ключевые слова*: циклотомические последовательности, $p$-адическая сложность.

Работа посвящена иследованию $p$-адической сложности ряда циклотомических и обобщенных циклотомических последовательностей. Периодическая автокорреляционная функция (ПАКФ), линейная сложность и $p$-адическая сложность являются важными характеристиками псевдослучайных последовательностей. Последовательности, обладающие высокой сложностью, представляют интерес для криптографических приложений. $p$-адическая сложность последовательности $\Phi(\mathbf{s})$ определяется как наименьшая длина регистра сдвига с обратной связью по переносу (feedback with carry shift register), порождающего последовательность. Симметричная $p$-адическая сложность определяется как $\overline{\Phi}(\mathbf{s}) = \min\left(\Phi(\mathbf{s}), \Phi(\widetilde{\mathbf{s}})\right)$, где $\widetilde{s} = (s_{N-1}, s_{N-2}, \ldots, s_0)$ [2]. В отличие от ПАКФ и линейной сложности, $p$-адическая сложность изучена только для ряда циклотомических или обобщенных циклотомических последовательностей. Основные работы посвящены исследованию 2-адической сложности бинарных последовательностей. В настоящий момент, известны только отдельные результаты о $p$-адической сложности последовательностей для $p \neq 2$. Так, $p$-адическая сложность бинарных последовательностей с периодом $2q$ изучена в [1], а 4-адическая сложность четвертичных последовательностей, также с периодом $2q$, в [3]. Таким образом, представляет интерес дальнейшее исследование $p$-адической сложности последовательностей, в том числе циклотомических и обобщенных циклотомических.

Пусть $q$ — нечетное простое число, $d > 1$ — натуральное число и $q \equiv 1 \pmod{d}$. Обозначим через $g$ примитивный корень по модулю $q$. Тогда циклотомические классы порядка $d$ по модулю $q$ определяются как

$$H_j = \left\{ g^{j+dt} \pmod{q} \,|\, 0 \leqslant t < (q-1)/d \right\}, \qquad j = 0, 1, \ldots, d-1.$$

Последовательности, сформированные с применением циклотомических классов, называются циклотомическими.

Разработана программа анализа $p$-адической сложности циклотомических и обобщенных циклотомических последовательностей. Исследована симметричная $p$-адическая сложность ряда последовательностей, определяемых по следующим правилам:

$$s_i = \begin{cases} 0, & \text{если } i \pmod{q} \in C_0, \\ 1, & \text{если } i \pmod{q} \in C_1. \end{cases} \quad \text{и} \quad u_i = \begin{cases} 0, & \text{если } i \pmod{q} \in H_0 \cup \{0\}, \\ j, & \text{если } i \pmod{q} \in H_j, \quad j = 1, \ldots, d-1. \end{cases}$$

Здесь $C_0$ и $C_1$ — разбиение $\mathbb{Z}_q$ посредством циклотомических классов. В результате, получены теоретические оценки для симметричной 2-адической сложности бинарных циклотомических последовательностей шестого порядка и для симметричной 4-адической сложности четвертичных циклотомических последовательностей четвертого порядка. Определено точное значение 3-адической сложности для троичных циклотомических последовательностей третьего порядка. Показано, что рассмотренные последовательности имеют высокую сложность. Ряд полученных результатов распространен на обобщенные циклотомические последовательности. Результаты расчетов подтверждают справедливость доказанных утверждений.

## СПИСОК ЛИТЕРАТУРЫ

1. *Jing X.*, *Xu Z.*, *Yang M.*, *Feng K.* On the $p$-Adic Complexity of the Ding-Helleseth-Martinsen Binary Sequences. — Chinese Journal of Electronics, 2021, v. 30, № 1, p. 64–71.
2. *Hu H.*, *Feng D.* On the 2-adic complexity and the k-error 2-adic complexity of periodic binary sequences. — IEEE Trans. Inf. Theory, 2008, v. 54, p. 874–883.
3. *Qiang S.*, *Li Y.*, *Yang M.*, *Feng K.* The 4-Adic Complexity of A Class of Quaternary Cyclotomic Sequences with Period $2p$. — arXiv:2011.11875v1 [cs.IT] 24 Nov 2020.

UDC 519.7

***Edemskiy V. A.*, *Churkin O. O.*, *Koltsova S. A.*** (Veliky Novgorod, Yaroslav-the-Wise Novgorod State University) . **About the symmetric $p$-adic complexity of cyclotomic and generalized cyclotomic sequences.**

*Abstract*: The $p$-adic complexity of a series of small-order cyclotomic sequences is studied. It is shown that these sequences have a high symmetric $p$-adic complexity. Separate results were obtained for generalized cyclotomic sequences.

*Keywords*: cyclotomic sequences, $p$-adic complexity.