О периодичности последовательностей Сомоса по модулю произвольного натурального числа

Устинов Алексей Владимирович
Национальный исследовательский университет “Высшая школа экономики”, г. Москва
ustinov.alexey@gmail.com
Секция: Теория чисел и дискретная математика

Для целого числа $k \geq 4$ последовательность Сомоса–k — это последовательность, порожденная квадратичным рекуррентным соотношением вида

$$s_{n+k}s_n = \sum_{j=1}^{[k/2]} \alpha_j s_{n+k-j}s_{n+j},$$

где α_j — константы, а $s_0, \ldots, s_{k-1}$ — начальные условия. Среди всех последовательностей Сомоса выделяется важный подкласс, обладающих различными нетривиальными свойствами. Это подкласс *последовательностей конечного ранга*. Последовательность $\{s_n\}_{n=-\infty}^{\infty}$ имеет (конечный) ранг r, если максимальный ранг двух бесконечных матриц

$$\left(s_{m+n}s_{m-n}\right)\Big|_{m,n=-\infty}^{\infty}, \qquad \left(s_{m+n+1}s_{m-n}\right)\Big|_{m,n=-\infty}^{\infty}$$

равен r. Если $r = 2$, то общий член последовательности Сомоса может быть выражен в терминах эллиптической функции. Общую последовательность конечного ранга можно рассматривать как последовательность, скрывающую за собой более сложную теорему сложения.

Доклад будет в посвящен доказательству периодичности целочисленных последовательностей конечного ранга по модулю произвольного натурального числа. В частности, это означает, что с помощью последовательностей конечного ранга можно строить криптографические протоколы, аналогичные тем, что строятся на эллиптических кривых.

Доклад будет сделан по результатам статьи [1].

Исследование выполнено за счет гранта Российского научного фонда № 22-41-05001, https://rscf.ru/project/22-41-05001/.

[1] А. В. Устинов, *О периодичности последовательностей Сомоса по модулю m*, Матем. заметки, 115:3 (2024), 439–449.