ЛИТЕРАТУРА

1. *Nyberg K.* Perfect nonlinear S-boxes // LNCS. 1991. V. 547. P. 378–386.
2. *Budaghyan L.* Construction and Analysis of Cryptographic Functions. Habilitation Thesis. University of Paris, 8 Sept. 2013.
3. *Туэкилин М. Э.* Почти совершенные нелинейные функции // Прикладная дискретная математика. 2009. № 3. С. 14–20.
4. *Городилова А. А.* Характеризация APN-функций через подфункции // Прикладная дискретная математика. Приложение. 2014. № 7. С. 15–16.
5. *McQuistan M. T., Wolfe A. J., Browning K. A., and Dillon J. F.* An APN permutation in dimension six // Amer. Math. Soc. 2010. No. 518. P. 33–42.
6. *Шушуев Г. И.* Векторные булевы функции на расстоянии один от APN-функций // Прикладная дискретная математика. Приложение. 2014. № 7. С. 36–37.

УДК 512.62

## ЗАДАЧА, ЭКВИВАЛЕНТНАЯ ПРОВЕРКЕ ПРОСТОТЫ ЧИСЕЛ ФЕРМА

Кр. Л. Геут, С. С. Титов

Работа посвящена постановке задачи, эквивалентной проверке простоты чисел Ферма. Сформулирована задача последовательного построения неприводимых многочленов над конечными полями характеристики два и три, эквивалентная проверке простоты чисел. Показана эквивалентность построения всех неприводимых симметричных многочленов степени $2^{k+1}$ над полем GF(2) и определения простоты числа Ферма $2^{2^k}$. Рассмотрена взаимосвязь между проверкой простоты чисел Ферма и построением неприводимых многочленов над GF(3).

**Ключевые слова:** *неприводимый многочлен, простые числа, числа Ферма.*

Неприводимые многочлены — аналог простых чисел — имеют большую ценность в теории информации, помехоустойчивом кодировании, работе конечных автоматов, стандартах защиты информации. Поэтому актуален поиск взаимосвязи между ними [1 – 4].

Интерес представляют многочлены степени $2^n$ над полем GF(2), коэффициенты которых при преобразовании в битовые строки широко используются для работы ЭВМ. В кодировании применяются симметричные (самовозвратные) многочлены [5] порядка $p = 2^{2^k} + 1$ степени $N = 2^{k+1}$. Легко показать, что если неприводимый над GF(2) многочлен имеет степень $2m$ и порядок $2^m + 1$, то он симметричен.

**Утверждение 1.** Простота числа Ферма $p = 2^{2^k} + 1$ эквивалентна равенству $p$ порядков всех неприводимых симметричных многочленов степени $n = 2^{k+1}$ над GF(2).

Так, например, при $k = 0$, $p = 3$ имеется один симметричный многочлен $x^2 + x + 1$ степени 2, порядка 3; при $k = 1$, $p = 5$ — один симметричный многочлен $x^4+x^3+x^2+x+1$ степени 4, порядка 5; при $k = 2$, $p = 17$ — два многочлена степени 8, порядка 17: $x^8 + x^7 + x^6 + x^4 + x^2 + x + 1$ и $x^8 + x^5 + x^4 + x^3 + 1$; при $k = 4$, $p = 65537$ имеется 2048 многочленов степени 32 порядка $p$ [6].

При $k = 5$ число $p = 4294967297 = 64 \cdot 6700417$ непростое, это означает, что неприводимые симметричные многочлены степени 64 имеют порядок 4294967297, или 641, или 6700417. Последовательным подбором коэффициентов были найдены 10 неприводимых симметричных многочленов степени 64 порядка 641 [4].

При $k = 6$ получаем $p = 18446744073709551617 = 274177 \cdot 67280421310721$. До настоящего времени не найдено простых чисел Ферма для $k > 4$, есть предположение, что их больше нет.

Как известно, круговой многочлен $x^{p-1} + \ldots + x + 1$ неприводим над полем $\mathrm{GF}(q)$ тогда и только тогда, когда $p$ простое и $q$ — первообразный корень по модулю $p$ [5]. Число Ферма $p$ простое тогда и только тогда, когда 3 — первообразный корень по модулю $p$ [7].

**Определение 1** [1, с. 55]. Пусть $P = F_q$, $K = \mathrm{GF}_{q^m}$ и $\alpha \in K$. След $\mathrm{Tr}_{K/P}(\alpha)$ элемента $\alpha$ из поля $K$ в поле $P$ определяется равенством $\mathrm{Tr}_{K/P}(\alpha) = \alpha + \alpha^q + \alpha^{q^2} + \ldots + \alpha^{q^{m-1}}$.

Переход от корней круговых многочленов при помощи функции следа к гауссовым нормальным базисам [1, с. 274] равносилен вычислению следа из поля $\mathrm{GF}(3^{2^s})$ в поле $\mathrm{GF}(3)$ корня уравнения $x^{p-1}+\ldots+x+1 = 0$ над $\mathrm{GF}(3^{2^s})$, $s = 2^k$, и даёт неприводимые многочлены над $\mathrm{GF}(3)$.

**Утверждение 2.** Пусть $p = 2^{2^k} + 1$ и $\zeta$ — корень кругового многочлена $\zeta^{p-1} + \zeta^{p-2} + \ldots + \zeta + 1 = 0$ над $\mathrm{GF}(3)$, так что $\zeta^p = 1$. Тогда простота числа $p$ эквивалентна неприводимости всех характеристических многочленов любого следа элемента $\zeta$.

**Утверждение 3.** Пусть $p$ — число Ферма. Тогда равенство следа элемента $\zeta \in \mathrm{GF}(3^{p-1})$ порядка $p$ в поле $\mathrm{GF}(3^2)$ корню $X = x$ неприводимого над $\mathrm{GF}(3)$ многочлена второй степени $X^2 + X + 2$ равносильно простоте числа $p$.

Таким образом, задача проверки простоты чисел Ферма эквивалентна построению многочленов над конечным полем $\mathrm{GF}(2)$ или $\mathrm{GF}(3)$ и проверке их на неприводимость.

## ЛИТЕРАТУРА


1. *Болотов А. А., Гашков С. Б., Фролов А. Б.* Элементарное введение в эллиптическую криптографию: алгебраические и алгоритмические основы. М.: КомКнига, 2006.
2. *Глуско Кр. Л., Титов С. С.* О квадратичных расширениях бинарных полей // Известия Российского государственного педагогического университета им. А. И. Герцена. 2013. № 154. С. 7–16.
3. *Геут Кр. Л., Титов С. С.* О поликвадратичном расширении бинарных полей // Прикладная дискретная математика. Приложение. 2013. № 6. С. 12–13.
4. *Геут Кр. Л., Титов С. С.* О генерации неприводимых многочленов простых порядков при построении дискретных устройств СЖАТиС // Транспорт Урала. 2014. № 1(40). С. 61–64.
5. *Лидл Р., Нидеррайтер Г.* Конечные поля. М.: Мир, 1988. 430 с.
6. *Геут К. Л., Титов С. С.* О генерации и применении неприводимых многочленов // III Информационная школа молодого ученого: сб. научных трудов. Екатеринбург, 2013. С. 293–298.
7. *Виноградов И. М.* Основы теории чисел. М.; Ижевск: НИЦ «Регулярная и хаотическая динамика», 2003. 176 с.