О функциях, выразимых полиномами по модулю квадрата простого числа

С. Н. Селезнева*

Получены свойства функций, выразимых полиномами по модулю квадрата простого числа, а также свойства замкнутого класса полиномов по модулю квадрата простого числа.

Ключевые слова: функция на конечном множестве, конечное кольцо, кольцо вычетов, полином, замкнутый класс.

Пусть $k \geqslant 2$, $E_k = \{0, 1, \ldots, k-1\}$, $P_k^{(n)} = \{f \mid f : E_k^n \to E_k\}$ — множество всех n-местных функций на E_k, $n \geqslant 1$, и $P_k = \bigcup\limits_{n \geqslant 1} P_k^{(n)}$. Пусть $Z_k = (E_k; +, -, \cdot)$ — кольцо вычетов по модулю k, где знаки $+$, $-$ и $\cdot$ обозначают сложение, вычитание и умножение по модулю k. Говорят, что полином $s \in Z_k[x_1, \ldots, x_n]$, $n \geqslant 1$, выражает функцию $f \in P_k^{(n)}$, если для любых $a_1, \ldots, a_n \in E_k$ верно $s(a_1, \ldots, a_n) = f(a_1, \ldots, a_n) (\mathrm{mod}\ k)$. Функция $f \in P_k^{(n)}$, $n \geqslant 1$, называется полиномиальной (по модулю k), если найдется полином $s \in Z_k[x_1, \ldots, x_n]$, который выражает функцию f. Пусть $Pol_k^{(n)}$ обозначает множество всех полиномиальных функций из $P_k^{(n)}$, $n \geqslant 1$, и $Pol_k = \bigcup\limits_{n \geqslant 1} Pol_k^{(n)}$. Множество Pol_k является замкнутым классом (клоном) относительно суперпозиции при любом числе k, $k \geqslant 2$ (см. [1,2]). При этом если k — простое число, то $Pol_k = P_k$; если k — составное число, то замкнутый класс Pol_k не является даже предполным [1]. В ряде работ найдены свойства функций из Pol_k и критерии полиномиальности функций из P_k, в частности, если k равно квадрату простого числа, см. [3–6] и др. В настоящей работе получены уточнения свойств функций, являющихся полиномиальными по модулю квадрата простого числа.

Пусть $k \geqslant 2$, $n \geqslant 1$. Если $a \in E_k^n$, то считаем, что $a = (a_1, \ldots, a_n)$, $i = 1, \ldots, n$. Если $a, b \in E_k^n$, $c, d \in E_k$, то $a + b = (a_1 + b_1, \ldots, a_n + b_n) \in E_k^n$, $c + da = (c + da_1, \ldots, c + da_n) \in E_k^n$. Положим $e_i = (\underbrace{0, \ldots, 0}_{i-1}, 1, \underbrace{0, \ldots, 0}_{n-i}) \in E_k^n$,

* *Селезнева Светлана Николаевна* — доктор физико-математических наук, профессор кафедры математической кибернетики факультета вычислительной математики и кибернетики Московского государственного университета имени М.В.Ломоносова, e-mail: selezn@cs.msu.ru.

Selezneva Svetlana Nikolaevna — Doctor of Sciences (Physics and Mathematics), Professor, Department of Mathematical Cybernetics, Faculty of Computational Mathematics and Cybernetics, Lomonosov Moscow State University.

Опубликовано на условиях лицензии CC-BY 4.0
Published under CC-BY 4.0

$i = 1, \ldots, n$. Пусть p — простое число, $m \geqslant 1$. Если $a \in E_p$, то положим $j_a(x) \in P^{(1)}_{p^m}$, где $j_a(b) = 1$ при $b = a(\mathrm{mod}\ p)$, иначе $j_a(b) = 0$, $b \in E_{p^m}$. Известно, что $j_a(x) = 1 - (x-a)^{\varphi(p^m)} \in Pol^{(1)}_{p^m}$, где $\varphi(p^m)$ — функция Эйлера. Если $n \geqslant 1$ и $a \in E^n_p$, то положим $j_a(x) = j_a(x_1, \ldots, x_n) = j_{a_1}(x_1) \cdot \ldots \cdot j_{a_n}(x_n) \in Pol^{(n)}_{p^m}$. Если z — переменная, принимающая значения из E_{p^2}, то $z = \delta_0(z) + p\delta_1(z)$, где $\delta_0, \delta_1 : E_{p^2} \to E_p$ — координатные функции переменной z (см. [3]). Если $z = (z_1, \ldots, z_n)$, $n \geqslant 1$, то положим $\delta_i(z) = (\delta_i(z_1), \ldots, \delta_i(z_n))$, $i = 0, 1$. Тогда $z = \delta_0(z) + p\delta_1(z)$. В следующих теоремах для упрощения записи для функций $f \in P^{(n)}_{p^2}$, $n \geqslant 1$, $f = f(z)$, вместо $\delta_0(z) + p\delta_1(z)$ пишем $x + py$, подразумевая $x = \delta_0(z)$, $y = \delta_1(z)$.

Теорема 1. *Пусть p — простое число, $n \geqslant 1$, $f \in P^{(n)}_{p^2}$ и для любого $a \in E^n_p$ верно $f(a + e_i p) - f(a) = 0(\mathrm{mod}\ p)$, где $e_i \in E^n_p$, $i = 1, \ldots, n$. Функция f — полиномиальна по модулю p^2 тогда и только тогда, когда для нее верно представление:*

$$f(x + py) \quad = \quad \sum_{a \in E^n_p} j_a(x)(f(a) + \sum_{i=1}^{n} (f(a + e_i p) - f(a))y_i).$$

Теорема 2. *Пусть p — простое число, $n \geqslant 1$, $f \in P^{(n)}_{p^2}$ и для любого $a \in E^n_p$ верно $f(a + e_i p) - f(a) = 0(\mathrm{mod}\ p)$, где $e_i \in E^n_p$, $i = 1, \ldots, n$. Функция f — полиномиальна по модулю p^2 тогда и только тогда, когда для любых $a, b \in E^n_p$ верно равенство:*

$$f(a + bp) \quad = \quad f(a) + \sum_{i=1}^{n} b_i (f(a + e_i p) - f(a)).$$

Теорема 3. *Пусть p — простое число, $n \geqslant 1$,*

$$N_{p^2}(n) = \{a, a + e_i p \mid a, e_i \in E^n_p, i = 1, \ldots, n\} \subseteq E^n_{p^2}.$$

Пусть $h \in P^{(n)}_{p^2}$ и функция h определена на множестве $N_{p^2}(n)$. Тогда найдется функция $f \in Pol^{(n)}_{p^2}$, совпадающая с функцией h на множестве $N_{p^2}(n)$, в том и только в том случае, когда для всех $a \in E^n_p$ и всех $i = 1, \ldots, n$ верны равенства $h(a + e_i p) - h(a) = 0(\mathrm{mod}\ p)$. При этом в том случае, когда функция f найдется, она однозначна.

Теорема 4. *Пусть p — простое число, $n \geqslant 1$, $f \in P^{(n)}_{p^2}$. Функция f — полиномиальна по модулю p^2 тогда и только тогда, когда для каждого $a \in E^n_p$ найдутся такие $d_a, c_{a,0}, c_{a,1}, \ldots, c_{a,n} \in E_p$, что для f верно представление:*

$$f(x + py) \quad = \quad \sum_{a \in E^n_p} j_a(x)(d_a + p(c_{a,0} + c_{a,1}y_1 + \ldots + c_{a,n}y_n)).$$

Полином $s \in Z_k[x_1, \ldots, x_n]$, $n \geqslant 1$, называется линейным, если $s(x_1, \ldots, x_n) = c_0 + c_1x_1 + \ldots + c_nx_n$, $c_0, c_1, \ldots, c_n \in E_k$. Функция $f \in P_k^{(n)}$, $n \geqslant 1$, называется линейной (по модулю k), если найдется линейный полином $s \in Z_k[x_1, \ldots, x_n]$, который выражает функцию f. Пусть $L_k^{(n)}$ обозначает множество всех линейных функций из $P_k^{(n)}$, $n \geqslant 1$, и $L_k = \bigcup\limits_{n \geqslant 1} L_k^{(n)}$. При любом числе k, $k \geqslant 2$, множество L_k является замкнутым классом (клоном) относительно суперпозиции, причем $L_k \neq P_k$. Кроме того, замкнутый класс L_k является предполным тогда и только тогда, когда k — простое число (см. [1, 2]).

Теорема 5. *Пусть p — простое число, $n \geqslant 1$. Тогда найдется взаимно однозначное отображение между множествами $Pol_{p^2}^{(n)}$ и $(L_p^{(n)} \times E_p)^{p^n}$, в частности, эти множества равномощны, т. е.*

$$|Pol_{p^2}^{(n)}| = p^{(n+2)p^n}.$$

Если $\rho \subseteq E_k^r$, $r \geqslant 0$, то ρ — отношение на E_k. Пусть R_k обозначает множество всех отношений на E_k. Если $S \subseteq R_k$, то, как обычно, $\mathrm{Pol}_k(S)$ обозначает множество всех функций из P_k, сохраняющих любое отношение из S (см. [2]). Пусть p — простое число. Положим $\rho_p \in R_{p^2}$, где $(a, b) \in \rho_p$ только при $a = b (\mathrm{mod}\ p)$, $a, b \in E_{p^2}$. Если $\sigma \in R_p$, $\sigma \subseteq E_p^r$, $r \geqslant 1$, то положим $\varphi(\sigma) = \tau \in R_{p^2}$, где $\tau = \bigcup\limits_{a \in E_p} (a + p\sigma) \subseteq E_{p^2}^r$, где $a + p\sigma = \{a + pc \mid c \in \sigma\} \subseteq E_{p^2}^r$, $a \in E_p$.

Теорема 6. *Пусть p — простое число, $S \subseteq R_p$ и $T = \bigcup\limits_{\sigma \in S} \varphi(\sigma) \subseteq R_{p^2}$. Если $\mathrm{Pol}_p(S) = L_p$, то $\mathrm{Pol}_{p^2}(T \cup \{\rho_p\}) = Pol_{p^2}$. Если $\mathrm{Pol}_{p^2}(T) = Pol_{p^2}$, то $\mathrm{Pol}_p(S) = L_p$.*

Исследование выполнено в рамках государственного задания МГУ имени М. В. Ломоносова.

Список литературы

[1] Яблонский С. В., “Функциональные построения в k-значной логике”, *Труды Математического института им. В.А. Стеклова АН СССР*, **51** (1958), 5–142.

[2] Lau D., *Function Algebras on Finite Sets*, Springer, Berlin, 2006, 671 pp.

[3] Ремизов А. Б., “О надструктуре замкнутого класса полиномов по модулю k”, *Дискретная математика*, **1**:1 (1989), 3–15.

[4] Мещанинов Д. Г., “Метод построения полиномов для функций k-значной логики”, *Дискретная математика*, **7**:3 (1995), 48–60.

[5] Селезнева С. Н., "О числе полиномиальных функций k-значной логики по составному модулю k", *Дискретная математика*, **28**:2 (2016), 81–91. DOI: 10.4213/dm1371.

[6] Селезнева С. Н., "Описание замкнутого класса полиномиальных функций по модулю квадрата простого числа посредством отношения", *Математические заметки*, **118**:4 (2025), 594–606. DOI: 10.4213/mzm14424.

Статья поступила 25 октября 2026 г.

On Functions Represented by Polynomials Modulo the Square of a Prime Number

S. N. Selezneva

Properties are obtained for functions represented by polynomials modulo the square of a prime number and for the closed class of polynomials modulo the square of a prime number.

Keywords: function on a finite set, finite ring, residue ring, polynomial, closed class.

References

[1] Yablonskiy S. V., "Functional constructions in a k-valued logic", *Tr. Mat. Inst. Steklova*, **51** (1958), 5–142.

[2] Lau D., *Function Algebras on Finite Sets*, Springer, Berlin, 2006, 671 pp.

[3] Remizov A. B., "Superstructure of the closed class of polynomials modulo k", *Discrete Mathematics and Applications*, **1**:1 (1991), 9–22. DOI: 10.1515/dma.1991.1.1.9.

[4] Meshchaninov D. G., "A method for constructing polynomials of k-valued logic functions", *Discrete Mathematics and Applications*, **5**:4 (1995), 333–346. DOI: 10.1515/dma.1995.5.4.333.

[5] Selezneva S. N., "On the number of functions of k-valued logic which are polynomials modulo composite k", *Discrete Mathematics and Applications*, **27**:1 (2017), 7–14. DOI: 10.1515/dma-2017-0002.

[6] Selezneva S. N., "Relational description of a closed class of polynomial functions modulo a squared prime", *Mathematical Notes*, **118**:3–4 (2025), 836–847. DOI: 10.1134/S0001434625605131.

Received on October 25, 2026