

*Пастухов Ю.Ф.<sup>1</sup> к.ф.-м.н., доцент кафедры  
технологий программирования*

*Пастухов Д.Ф.<sup>1</sup> к.ф.-м.н., доцент кафедры  
технологий программирования*

*Косарев И.Ю.<sup>2</sup> аспирант*

*Пастухов А.Ю.<sup>3</sup> магистрант*

## **О КРИТЕРИИ АЛГЕБРАИЧЕСКИХ ВЫЧЕТОВ И НЕВЫЧЕТОВ ОДИННАДЦАТОГО ПОРЯДКА В ПОЛЕ ВЫЧЕТОВ $Z_p$**

<sup>1</sup>Полоцкий государственный университет имени Евфросинии Полоцкой, Полоцк, Беларусь

<sup>2</sup>Московский автомобильно-дорожный государственный технический университет (МАДИ),  
Москва, Россия

<sup>3</sup>Витебский государственный университет имени П.М. Машерова

### **Аннотация.**

Алгебраические вычеты и невычеты одиннадцатого порядка (степени) в поле  $Z_p$  – элементы этого поля  $Z_p$  для которых существует хотя бы одно решение простейшего (канонического) уравнения одиннадцатой с коэффициентом при старшем члене, равном 1, и свободным членом, равным данному(фиксированному) элементу поля  $Z_p$ .

Критерий вычетов одиннадцатой степени (порядка) выводится из критерия существования алгебраического уравнения степени  $n$ .

Вычеты и невычеты одиннадцатого порядка используются в теории чисел, алгебре, теории групп, существовании корней алгебраических уравнений, криптографии компьютерной и информационной безопасности.

### **1. Введение.**

В работе [2] был получен результат-критерий (теорема1) существования наличия решений алгебраических уравнений в кольце вычетов  $Z_m$ , с образующими и свободным членом, наибольший общий делитель которого с порядком, равен единице (взаимно прост с порядком кольца).

В данной работе сформулирован критерий вычетов одиннадцатой степени (порядка) из общего факта [2].

По определению в криптологии, криптографии и алгебре, алгебраические вычеты одиннадцатого порядка(степени) в поле  $Z_p$  – это такие элементы  $a \in Z_p$ , что найдется(существует) хотя бы одно решения уравнения  $x^{11} \equiv a \pmod{p}$ , алгебраические невычеты одиннадцатого порядка(степени) в поле  $Z_p$  – это такие элементы поля вычетов  $a \in Z_p$ , для которых нет(пустое множество) решения уравнения  $x^{11} \equiv a \pmod{p}$  Количество образующих элементов(генераторов) равно  $\varphi(\varphi(m))$ , где  $\varphi$  – функция Эйлера.

Как известно из алгебры

$Z_m^*$  – циклическая  $\Leftrightarrow$  1)  $m = 2$  2)  $m = 4$  3)  $m = p^k$  4)  $m = 2p^k$  (в 3), 4)  $p$  – нечетное простое)

**Теорема 1. (Критерий вычетов одиннадцатого порядка(степени) в поле  $Z_p$ )**

Предположим, что  $Z_p$  – поле вычетов по простому нечетному модулю  $p$ . И пусть  $g$  – произвольный порождающий (генератор) элемент поля  $Z_p$  (один такой элемент непременно есть, так как  $p$  – простое). Тогда:

1)  $a = 0$  является вычетом десятого порядка (степени) (поскольку есть очевидное решение  $x = 0$ :  $0^{11} = 0 \pmod{p}$ )

2)  $a \neq 0$  пусть

$$a \neq 0 \Rightarrow a \in Z_p^* \Rightarrow \exists 1 \leq \beta \leq \varphi(p) = p-1: a = g^\beta \Leftrightarrow \beta = \log_g a \quad (1)$$

$a$  – вычет 11-ой порядка(степени) в

$$Z_p \Leftrightarrow \beta = \log_g a \equiv 0 \pmod{\text{НОД}(\varphi(p) = p-1, n=11)} \Leftrightarrow \beta \text{ делится нацело (без остатка) на } \text{НОД}(p-1, 11) \quad (2)$$

$$\text{НОД}(p-1, 11) = \begin{cases} 11, \text{при } p = 11k + 1(a) \\ 1, \text{при } p \neq 11k + 1(b) \Leftrightarrow \\ \text{то есть, при } p = 11k \text{ или } p = 11k + 2 \text{ или } p = 11k + 3 \text{ или } p = 11k + 4(c) \\ \text{или при } p = 11k + 5 \text{ или } p = 11k + 6 \text{ или } p = 11k + 7 \text{ или } p = 11k + 8 \\ \text{или при } p = 11k + 9 \text{ или } p = 11k + 10 \end{cases} \quad (3)$$

Условие (2) не зависит от выбора образующего(порождающего) элемента поля вычетов.

**Пример 1.** Рассмотрим для примера кольцо по нечетному простому модулю  $Z_{p=7}$ , количество генераторов(образующих) в  $Z_7$   $\varphi(\varphi(m=7)) = \varphi(6) = 2$ , найдем их

Порождающие(образующие) поля  $Z_{p=7}$  это  $\{3, 5\}$ :

$$\{3^1 \equiv 3 \pmod{7}, 3^2 \equiv 2 \pmod{7}, 3^3 \equiv 6 \pmod{7}, 3^4 \equiv 4 \pmod{7}, 3^5 \equiv 5 \pmod{7}, 3^6 \equiv 1 \pmod{7}\} \Rightarrow g = 3 \text{ – образующий}$$

$$\{5^1 \equiv 5 \pmod{7}, 5^2 \equiv 4 \pmod{7}, 5^3 \equiv 6 \pmod{7}, 5^4 \equiv 2 \pmod{7}, 5^5 \equiv 3 \pmod{7}, 5^6 \equiv 1 \pmod{7}\} \Rightarrow g = 5 \text{ – образующий}$$

Для иллюстрации применения сформулированной выше факта рассмотрим, как пример для применения, образующий  $g = 3$

$$\log_{g=3}(a=2) = \beta = 2 \Leftrightarrow 3^2 \equiv 2 \pmod{7}, \log_{g=3}(a=3) = \beta = 1 \Leftrightarrow 3^1 \equiv 3 \pmod{7}, \log_{g=3}(a=5) = \beta = 5 \Leftrightarrow 3^5 \equiv 5 \pmod{7}$$

$$\log_{g=3}(a=1) = \beta = 6 \Leftrightarrow 3^6 \equiv 1 \pmod{7}, \log_{g=3}(a=4) = \beta = 4 \Leftrightarrow 3^4 \equiv 4 \pmod{7}, \log_{g=3}(a=6) = \beta = 3 \Leftrightarrow 3^3 \equiv 6 \pmod{7}$$

По критерию (теорема 1)

$\beta = 2, 1, 5, 6, 4, 3$  делится на  $\text{НОД}(p-1=7-1=6, 11)=1$  следовательно  $a = 2, 3, 5, 6, 4, 3$  – вычеты. Ну, и, конечно, очевидный вычет 0, являющийся вычетом любого конечного порядка в любом кольце (пункт 1) теоремы 1).

Рассмотрим далее другой образующий элемент поля  $Z_{p=7}$  образующий  $g = 5$

$$\log_{g=5}(a=2) = \beta = 4 \Leftrightarrow 5^4 \equiv 2 \pmod{7}, \log_{g=5}(a=3) = \beta = 5 \Leftrightarrow 5^5 \equiv 3 \pmod{7}, \log_{g=5}(a=5) = \beta = 1 \Leftrightarrow 5^1 \equiv 5 \pmod{7}$$

$$\log_{g=5}(a=1) = \beta = 6 \Leftrightarrow 5^6 \equiv 1 \pmod{7}, \log_{g=5}(a=4) = \beta = 2 \Leftrightarrow 5^2 \equiv 4 \pmod{7}, \log_{g=5}(a=6) = \beta = 3 \Leftrightarrow 5^3 \equiv 6 \pmod{7}$$

По критерию (**теорема 1**)  $\beta = 4, 5, 1, 6, 2, 3$  делится на  $\text{НОД}(p-1=7-1=6, 11)=1$  следовательно,  $a = 2, 3, 5, 1, 4, 6$  – вычеты, и, конечно же, вычет 0 (пункт 1 **теоремы 1**), который будет вычетом любого конечного порядка(степени) в любом кольце.

Это иллюстрируют следующие вычисления:

$$\{0^{11} \equiv 0(\bmod 7), 1^{11} \equiv 1(\bmod 7), 2^{11} \equiv 4(\bmod 7), 3^{11} \equiv 5(\bmod 7), 4^{11} \equiv 2(\bmod 7), 5^{11} \equiv 3(\bmod 7), 6^{11} \equiv 6(\bmod 7)\}$$

Из последней строки вычислений видно, что в кольце  $Z_7$  все элементы кольца являются вычетами 11-й степени (невыветов 11-й степени – нет)

#### **Список использованных источников:**

1. Волосова Н.К., Волосов К.А., Волосова А.К., Карлов М.И., Пастухов Д.Ф., Пастухов Ю.Ф. Обобщение метода Петрова - Галеркина для решения системы интегральных уравнений Фредгольма второго рода // Вестник Пермского университета. Математика. Механика. Информатика. 2023. № 1(60). С. 5–14.
2. Пастухов Ю.Ф., Пастухов Д.Ф., Чернов С.В., Волосова Н.К., Волосов К.А., Волосова А.К. Критерий существования решений, количество решений, структура решений канонического неоднородного алгебраического уравнения степени  $n$  в кольце вычетов  $Z_m$  с генераторами и свободным членом, взаимно простым с порядком кольца // Тенденции развития науки и образования. 2023. № 101-4. С. 114–117.
3. Волосова Н.К., Волосов К.А., Волосова А.К., Пастухов Д.Ф., Пастухов Ю.Ф. Обобщение формулы Эйлера для непланарного графа. Москва, 2024.
4. Волосова Н.К., Волосов К.А., Волосова А.К., Карлов М.И., Пастухов Д.Ф., Пастухов Ю.Ф. Модифицированная формула Герасимова - Капуто // Вестник Пермского университета. Математика. Механика. Информатика. 2024. № 1(64). С. 5–14.
5. Волосова Н.К., Волосов К.А., Волосова А.К., Пастухов Д.Ф., Пастухов Ю.Ф., Сеница П.Р. Шифрование данных на базе эллиптических кривых. Учебное пособие / Москва, 2023.