УДК 511; 512; 003.326

КРИТЕРИЙ, КОЛИЧЕСТВО И СТРУКТУРА КВАДРАТИЧНЫХ ВЫЧЕТОВ И НЕВЫЧЕТОВ В ПОЛЕ Z_P В ТЕРМИНАХ ОБРАЗУЮЩИХ ЭЛЕМЕНТОВ – ВЫВОД ИЗ КРИТЕРИЯ СУЩЕСТВОВАНИЯ РЕШЕНИЙ КАНОНИЧЕСКОГО НЕОДНОРОДНОГО АЛГЕБРАИЧЕСКОГО УРАВНЕНИЯ СТЕПЕНИ *n* В КОЛЬЦЕ ВЫЧЕТОВ С ГЕНЕРАТОРАМИ И СВОБОДНЫМ ЧЛЕНОМ, ВЗАИМНО ПРОСТЫМ С ПОРЯДКОМ КОЛЬЦА

канд. физ.-мат. наук Ю. Ф. ПАСТУХОВ[1], канд. физ.-мат. наук Д. Ф. ПАСТУХОВ[1], д-р физ.-мат. наук, проф. К. А. ВОЛОСОВ[4], С. В. ЧЕРНОВ[2], А. Ю. ПАСТУХОВ[3], канд. физ.-мат. наук А. К. ВОЛОСОВА[4], Н. К. ВОЛОСОВА[5], В. А. МАКАРЫЧЕВА[1], М. Ю. МАКАРЫЧЕВ[1]

[1](Полоцкий государственный университет имени Евфросинии Полоцкой, Беларусь)

[2](Конструкторское бюро «Дисплей», г. Витебск, Беларусь)

[3](Витебский государственный университет имени П. М. Машерова, Беларусь)

[4](РУТ(МИИТ) Московский государственный университет путей сообщения Императора Николая II, Россия)

[5](МГТУ им. Н. Э. Баумана, г. Москва, Россия)

Аннотация. *Квадратичные вычеты и невычеты в поле – элементы поля для которых существует решение квадратного уравнения с единичным коэффициентом при старшем члене, отсутствующем члене с первой степенью и свободным членом, равным рассматриваемому элементу поля вычетов по простому модулю. Критерий и структура квадратичных вычетов получены из более общего критерия существования алгебраического уравнения степени n. Квадратичные вычеты и невычеты используются в теории чисел криптографии и входят в программы курсов криптологии и криптографии для студентов по специальности компьютерная безопасность.*

Ключевые слова: *элементы поля, квадратичный вычет, решение квадратного уравнения, критерия существования алгебраического уравнения.*

Введение. В работе [1] исследовался вопрос о существовании решений алгебраических уравнений в кольце вычетов Z_m в результате – получен мощный и эффективный инструмент исследования существования решений – сформулирована и доказана теорема 1 – критерий существования (канонического) алгебраического уравнения степени n в кольце вычетов Z_m с образующими и свободным членом, взаимно простым с порядком кольца.

Новым в данной работе является получение нового критерия о квадратичных вычетах и невычетах из более общего критерия существования решения канонического неоднородного алгебраического уравнения степени n в кольце вычетов Z_m специального типа – с образующими и свободным членом, взаимно простым с порядком кольца то есть в кольцах, у которых мультипликативная группа является циклической. Поскольку мультипликативная группа поля Z_p Z_p^* состоит из всех ненулевых элементов и является циклической, так как p – простое, то это обстоятельство создает идеальное условие для применения более общего критерия.

Как известно, вычеты в поле Z_p – это такие элементы $a \in Z_p$, для которых существуют решения уравнения $x^2 \equiv a(\mathrm{mod}\, p)$, невычеты в поле Z_p – это такие элементы $a \in Z_p$, для которых не существуют решения уравнения $x^2 \equiv a(\mathrm{mod}\, p)$. Количество всех образующих в кольце Z_m равно $\varphi(\varphi(m))$, где φ – функция Эйлера.

Известно также, что

$$Z_m^* \text{ – циклическая} \Leftrightarrow 1)\ m = 2,\ 2)\ m = 4,\ 3)\ m = p^k,$$
$$4)\ m = 2p^k, (k \in Z),\ p \text{ – нечетное простое } (p \geq 3).$$

Полученный критерий квадратичных вычетов и соответственно невычетов **кардинально отличается** от известного критерия квадратичных вычетов и невычетов Леонарда Эйлера:

$$a \text{ – квадратичный вычет} \Leftrightarrow a^{\frac{p-1}{2}} \equiv 1(\mathrm{mod}\, p).$$

Прямым и очевидным следствием **Теоремы 1** из [1] является следующая теорема:

Теорема 1 (Критерий, количество и структура квадратичных вычетов и невычетов в поле Z_p)

Пусть Z_p – поле вычетов по простому модулю p. Пусть g – произвольный образующий поля Z_p (хотя бы один такой элемент обязательно существует так как p – простое). Тогда:

1) $a = 0$ является квадратичным вычетом (так как существует очевидное решение $x = 0 : 0^2 = 0(\mathrm{mod}\, p)$);

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

a – квадратичный вычет в $Z_p \Leftrightarrow \beta = \log_g a \equiv 0$ $(\text{НОД}(\varphi(p) = p - 1, n = 2)) \Leftrightarrow \beta$ делится без остатка на $\text{НОД}(p - 1, 2)$ (2).

$\text{НОД}(p - 1, 2) = \begin{cases} \mid 1, \text{при } p = 2 \\ \mid 2, \text{при } p > 2 \end{cases}$ (3). Условие (2) инвариантно относительно выбора образующего.

3) структура квадратичных вычетов и невычетов. Все квадратичные вычеты для простых $p>2$ (нечетных) имеют вид $a_0=0,\ a_k=g^{2k}$, где $k=\overline{1,\frac{\varphi(p)=p-1}{2}}$.

Все квадратичные невычеты имеют вид $a_k=g^{2k+1}$, где $k=\overline{1,\frac{\varphi(p)=p-1}{2}}$.

4) количество квадратичных вычетов $\frac{p-1}{2}+1=\frac{p+1}{2}$, невычетов – $\frac{p-1}{2}$.

Пояснение к формуле (3) – очевидно, что для простых $p>2$, p – простое $\Rightarrow$ $p-1\geq 2$ и $p-1\equiv 0(\mathrm{mod}\,2)$ $\Rightarrow$ НОД$(p-1,2)=2$. Если $p=2$ $\Rightarrow$ НОД$(p-1,2)=$ $=$НОД$(1,2)=1$ $\Rightarrow$ в $Z_2=\{0,1,+,*\}$ $\Rightarrow$ $g^{\beta}=1^1\equiv 1(\mathrm{mod}\,2)$ $\Rightarrow$ $\log_{g=1}1=1$ $\Rightarrow$ $\beta=1$ $a=1$ – вычет ($1^2=1\equiv 1(\mathrm{mod}\,p=2)$) и по критерию $\beta=1\equiv 0$ (НОД$(p-1,2)=$НОД$(1,2)=1$) – также вычет.

Пример 1. Рассмотрим для примера кольцо по простому модулю $\boldsymbol{Z_5}$, количество образующих в $\boldsymbol{Z_5}$ $\varphi(\varphi(m=5))=\varphi(4)=2$, найдем их.

Образующие кольца $\boldsymbol{Z_5}$ это $\{2,3\}$: $\{2^1=2\equiv 2(\mathrm{mod}\,5),\ 2^2=4\equiv 4(\mathrm{mod}\,5),$ $2^3=8\equiv 3(\mathrm{mod}\,5),\ 2^4=16\equiv 1(\mathrm{mod}\,5)\}$ $\Rightarrow$ $g=2$ – образующий. $\{3^1=3\equiv 3(\mathrm{mod}\,5),$ $3^2=9\equiv 4(\mathrm{mod}\,5),\ 3^3=27\equiv 2(\mathrm{mod}\,5),\ 3^4=81\equiv 1(\mathrm{mod}\,5)\}$ $\Rightarrow$ $g=3$ – образующий. Рассмотрим, например, образующий $g=2$.

$$\log_{g=2}a=2=\beta=1\Leftrightarrow 2^1\equiv 2(\mathrm{mod}\,5),$$
$$\log_{g=2}a=3=\beta=3\Leftrightarrow 2^3\equiv 3(\mathrm{mod}\,5).$$

По критерию **(теорема 1)** ни 1, ни 3 не делится на 2, следовательно, 2, 3 – невычеты.

$$\log_{g=2}a=1=\beta=4\Leftrightarrow 2^4\equiv 1(\mathrm{mod}\,5),$$
$$\log_{g=2}a=4=\beta=2\Leftrightarrow 2^2\equiv 4(\mathrm{mod}\,5).$$

По критерию **(теорема 1)** как 2 так и 4 делится на 2, следовательно 1, 4 – вычеты, ну и,конечно, тривиальный вычет 0, который является вычетом произвольной степени в любом кольце.

Рассмотрим, например, образующий $g=3$.

$$\log_{g=3}a=2=\beta=3\Leftrightarrow 3^3\equiv 2(\mathrm{mod}\,5),$$
$$\log_{g=3}a=3=\beta=1\Leftrightarrow 3^1\equiv 3(\mathrm{mod}\,5).$$

По критерию **(теорема 1)** ни 1, ни 3 не делится на 2 следовательно 2, 3 – невычеты.

$$\log_{g=3} a = 1 = \beta = 4 \Leftrightarrow 3^4 \equiv 1(\mathrm{mod}\,5),$$

$$\log_{g=3} a = 4 = \beta = 2 \Leftrightarrow 3^2 \equiv 4(\mathrm{mod}\,5).$$

По критерию **(теорема 1)** как 2 так и 4 делится на 2, следовательно 1, 4 – вычеты, ну и,конечно, тривиальный вычет 0, который является вычетом произвольной степени в любом кольце.

По **теореме 1, пункт 3** вычеты:

$$g = 22^{2*1} \equiv 4(\mathrm{mod}\,5) 2^{2*2} \equiv 1(\mathrm{mod}\,5),$$

$$g = 33^{2*1} \equiv 4(\mathrm{mod}\,5) 3^{2*2} \equiv 1(\mathrm{mod}\,5).$$

По **теореме 1, пункт 3** невычеты:

$$g = 22^{2*1+1} \equiv 3(\mathrm{mod}\,5) 2^{2*2+1} \equiv 2(\mathrm{mod}\,5),$$

$$g = 33^{2*1+1} \equiv 2(\mathrm{mod}\,5) 3^{2*2+1} \equiv 3(\mathrm{mod}\,5).$$

Как и положено быть.

ЛИТЕРАТУРА

1. Пастухов, Ю. Ф. Критерий существования решений, количество решений, структура решений канонического неоднородного алгебраического уравнения степени n в кольце вычетов Zm с генераторами и свободным членом, взаимно простым с порядком кольца / Ю.Ф. Пастухов, Д.Ф. Пастухов, С.В. Чернов, Н.К. Волосова, К.А. Волосов, А.К. Волосова // Тенденции развития науки и образования. – 2023. – № 101-4. – С. 114–117.