Пастухов Юрий Феликсович
Пастухов Дмитрий Феликсович
Полоцкий государственный университет
имени Евфросинии Полоцкой, Полоцк, Республика Беларусь,
Полоцкий государственный университет
conference1900mail.ru, dmitrij.pastuhov@mail.ru

Биквадратичные вычеты в поле Z_p

Биквадратичные вычеты Z_p — элементы поля, для которых существует решение канонического уравнения 4-ой с единичным коэффициентом при старшем члене и свободным членом, совпадающим с заданным элементом поля.

Критерий и структура вычетов может быть получен из критерия существования алгебраического уравнения степени n.

Биквадратичные вычеты используются в алгебре, теории чисел, компьютерной безопасности криптологии, криптографии, информационной безопасности.

Ключевые слова: вычеты, невычеты, существование решения, алгебраическое уравнение, кольцо вычетов.

ВВЕДЕНИЕ

В работе [Критерий существования решений, 2023, с. 115] 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. О вычетах 3-ей степени можно прочитать в [Пастухов, 2024, с. 156].

Новым в данной работе является структура биквадратичных — 4-й степени вычетов из более общего критерия [Критерий существования решений, 2023, с. 115] существования решения канонического неоднородного алгебраического уравнения степени в кольцах вычетов с генераторами. Так как мультипликативная группа поля Z_p Z_p^* состоит из всех ненулевых элементов и является циклической и так как p — простое, это обстоятельство создает уникальное условие для применения более общего критерия.

Известно, вычеты в поле Z_p — это такие элементы $a \in Z_p$, для которых существуют решения уравнения $x^4 \equiv a \,(\mathrm{mod\,p})$, невычеты в поле Z_p — это такие элементы $a \in Z_p$, для которых не существуют решения

уравнения $x^4 \equiv a(\mathrm{mod\,p})$. Количество порождающих равно φ(φ(m)), где φ – функция Эйлера.

Из алгебры известно, что

$$Z_m^* - \textit{циклическая} \Leftrightarrow 1)\, m = 2 \;\; 2) m = 4 \;\; 3) m = p^k$$
$$4) m = 2p^k (\textit{в } 3), 4) \;\; p - \textit{нечетное простое})$$

Элементы кольца 0 и 1 всегда являются вычетами любой степени в кольце любого конечного порядка. Интерес представляет вопрос, как устроены все вычеты, например, 4-ой степени? Есть ли то общее, что их объединяет? Ответ на этот вопрос дает следующая

Теорема 1 (Строение (структура) биквадратичных вычетов в поле Z_p)

Пусть Z_p – поле вычетов по простому нечетному модулю p. Пусть g – произвольный порождающий элемент поля Z_p (хотя бы один такой элемент обязательно существует, так как $p-$ простое), тогда:

1) $a = 0$ является кубическим вычетом (так как существует очевидное решение $x = 0$: $0^3 = 0(\mathrm{mod\,p})$)

2) в случае $a \neq 0$ все вычеты 4-й степени имеют вид:

$$a_0 = 0,\; a_k = g^{НОД(p-1,4)*k} \;\; k = \overline{1, \frac{p-1}{НОД(p-1,4)}}$$

3) Количество вычетов равно в случае равно $\frac{p-1}{НОД(p-1,4)} + 1$ (прибавление 1 в формуле — это учет тривиального вычета 0).

Пример 1. В этом примере рассмотрим поле Z_5. Этот пример интересен тем, что в этом случае есть только тривиальные вычеты — 0 и 1. Количество образующих в Z_5 $\varphi(\varphi(\mathrm{m} = 5)) = \varphi(4) = 2$, определим их.

Образующие кольца — это $\{2,3\}$:

$$\left\{2^1 \equiv 2(\mathrm{mod}\,5), 2^2 \equiv 4(\mathrm{mod}\,5), 2^3 \equiv 3(\mathrm{mod}\,5), 2^4 \equiv 1(\mathrm{mod}\,5)\right\} \Rightarrow g = 2 - \textit{образующий}$$
$$\left\{3^1 \equiv 3(\mathrm{mod}\,5), 3^2 \equiv 4(\mathrm{mod}\,5), 3^3 \equiv 2(\mathrm{mod}\,5), 3^4 \equiv 1(\mathrm{mod}\,7)\right\} \Rightarrow g = 3 - \textit{образующий}$$

Рассмотрим, например, *образующий* $g = 2$

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

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

По теореме 1 вычеты $НОД(p-1,4)=НОД(5-1,4)=НОД(4,4)=4$,

$$a_k=g^{НОД(p-1,4)*k}=g^{НОД(5-1,4)*k}=g^{4*k}\quad k=1,\overline{\frac{p-1}{НОД(p-1,4)}}=\overline{1},$$

$$\overline{\frac{5-1}{НОД(5-1,4)}}=1,\overline{\frac{5-1}{4}}=\overline{1,1}$$

то есть вычеты — это: $a_{k=1}=g^{НОД(p-1,4)*k}=g^{4*1}=g^4=2^4\equiv 1(\mathrm{mod}\,5)$

Значит, у нас всего 1 ненулевой вычет — это 1, и разумеется, 0.

Рассмотрим другой *образующий* $g = 3$

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

По теореме 1 вычеты $НОД(p-1,4)=НОД(7-1,4)=НОД(6,4)=2$,

$$a_k=g^{НОД(p-1,4)*k}=g^{НОД(5-1,4)*k}=g^{4*k}$$

$$k=1,\overline{\frac{p-1}{НОД(p-1,4)}}=1,\overline{\frac{5-1}{НОД(5-1,4)}}=1,\overline{\frac{5-1}{4}}=\overline{1,1}$$

то есть вычеты — это: $a_{k=1}=g^{НОД(p-1,4)*k}=g^{4*1}=g^4=3^4\equiv 1(\mathrm{mod}\,5)$

поэтому опять получаем биквадратичные вычеты — это 0,1.

Это действительно так, как показывают простые вычисления, приведенные ниже:

$$\left\{0^4\equiv 0(\mathrm{mod}\,5),1^4\equiv 1(\mathrm{mod}\,5),2^4\equiv 1(\mathrm{mod}\,5),3^4\equiv 1(\mathrm{mod}\,5),4^4\equiv 1(\mathrm{mod}\,5)\right\}$$

Оказывается, в некоторых полях Z_p есть только тривиальные вычеты 4-й степени –это 0,1.

Все остальные элементы — невычеты. Этот результат существенно отличается от случая $p = 2$.

Пример 2. Для примера рассмотрим кольцо по нечетному простому модулю Z_p, количество образующих в Z_7 $\varphi(\varphi(m=7))=\varphi(6)=2$, найдем их.

Образующие кольца — это $\{3,5\}$:

$$\left\{3^1\equiv 3(\bmod 7), 3^2\equiv 2(\bmod 7), 3^3\equiv 6(\bmod 7), 3^4\equiv 4(\bmod 7), 3^5\equiv 5(\bmod 7)\right\}\Rightarrow$$

$$g=2 \text{ — } \textit{образующий}$$

$$\left\{5^1\equiv 5(\bmod 7), 5^2\equiv 4(\bmod 7), 5^3\equiv 6(\bmod 7), 5^4\equiv 2(\bmod 7), 5^5\equiv 3(\bmod 7)\right\}\Rightarrow$$

$$g=5 \text{ — } \textit{образующий}$$

Рассмотрим, например, *образующий* $g=3$

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

$$\log_{g=3}(a=5)=\beta=5\Leftrightarrow 3^5\equiv 5(\bmod 7)$$

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

$$\log_{g=3}(a=6)=\beta=3\Leftrightarrow 3^3\equiv 6(\bmod 7)$$

По теореме1 вычеты $НОД(p-1,4)=НОД(7-1,4)=НОД(6,2)=2$,

$$a_k=g^{НОД(p-1,4)*k}=g^{НОД(7-1,4)*k}=g^{2*k}$$

$$k=\overline{1,\frac{p-1}{НОД(p-1,4)}}=\overline{1,\frac{7-1}{НОД(7-1,4)}}=\overline{1,\frac{7-1}{2}}=\overline{1,3}$$

то есть вычеты — это: $a_{k=1}=g^{НОД(p-1,4)*k}=g^{2*1}=g^2=5^2\equiv 4(\bmod 7)$

$$a_{k=2}=g^{НОД(p-1,4)*k}=g^{2*2}=g^4=5^4\equiv 2(\bmod 7).$$

$$a_{k=3}=g^{НОД(p-1,4)*k}=g^{2*3}=g^6=5^6\equiv 1(\bmod 7)$$

Значит, вычеты — это 2,4,1, и конечно, 0.

Рассмотрим, например, *образующий* $g=5$

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

$$\log_{g=5}(a=5)=\beta=1\Leftrightarrow 5^1\equiv 5(\bmod 7)$$

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

$$\log_{g=5}(a=6)=\beta=3\Leftrightarrow 5^3\equiv 6(\bmod 7)$$

По теореме 1 вычеты $НОД(p-1,4) = НОД(7-1,4) = НОД(6,2) = 2$,

$$a_k = g^{НОД(p-1,4)*k} = g^{НОД(7-1,4)*k} = g^{2*k}$$

$$k = \overline{1,\frac{p-1}{НОД(p-1,4)}} = \overline{1,\frac{7-1}{НОД(7-1,4)}} = \overline{1,\frac{7-1}{2}} = \overline{1,3},$$

то есть вычеты — это: $a_{k=1} = g^{НОД(p-1,4)*k} = g^{2*1} = g^2 = 5^2 \equiv 4(\mathrm{mod}\,7)$

$$a_{k=2} = g^{НОД(p-1,4)*k} = g^{2*2} = g^4 = 5^4 \equiv 2(\mathrm{mod}\,7)$$

$$a_{k=3} = g^{НОД(p-1,4)*k} = g^{2*3} = g^6 = 5^6 \equiv 1(\mathrm{mod}\,7),$$

поэтому опять получаем биквадратичные вычеты– это 4,2,1, и конечно, 0.

Это соответствует действительности, как показывают следующие расчеты:

$$\{0^4 \equiv 0(\mathrm{mod}\,7), 1^4 \equiv 1(\mathrm{mod}\,7), 2^4 \equiv 2(\mathrm{mod}\,7), 3^4 \equiv 4(\mathrm{mod}\,7), 4^4 \equiv 4(\mathrm{mod}\,5),$$

$$5^4 \equiv 2(\mathrm{mod}\,7), 6^4 \equiv 1(\mathrm{mod}\,7)\}$$

ЛИТЕРАТУРА

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 / Ю. Ф. Пастухов, Д. Ф. Пастухов, С. В. Чернов [и др.] // Тенденции развития науки и образования. 2023. № 101–4. С. 114–117. https://doi.org/10.18411/trnio-09–2023–186.

Критерий, количество и структура кубических вычетов в поле Z_p / Ю. Ф. Пастухов, Д. Ф. Пастухов, К. А. Волосов [и др.] // Вопросы обеспечения безопасности в киберпространстве : Материалы II Всероссийской научно-технической конференции, Махачкала, 10–11 мая 2024 года. — Махачкала: Типография ФОРМАТ, 2024. — С. 156–158. — EDN LCHKCJ.

Pastukhov Yu. F., Pastukhov D. F.
Euphrosyne Polotskaya State University of Polotsk,
Polotsk, Belarus

Biquadratic deductions in the Z_p field

Biquadratic residues are elements of a field for which there is a solution of the canonical equation of the 4th with a unit coefficient for the highest term and a free term coinciding with a given element of the field.

The criterion and structure of the deductions can be obtained from the criterion of the existence of an algebraic equation of degree n.

Biquadratic deductions are used in algebra, number theory, computer security, cryptology, cryptography, and information security.

Keywords: deductions, non-deductions, existence of a solution, algebraic equation, ring of deductions.

Подходова Наталья Семеновна
Российский государственный педагогический
университет им. А. И. Герцена, Санкт-Петербург, Россия
podhodova@gmail.com
Соколова Анастасия Денисовна
Государственное бюджетное общеобразовательное учреждение
гимназия № 278 имени Б. Б. Голицына
Адмиралтейского района, Санкт-Петербург, Россия
sokolan290@gmail.com

Задания на создание учебной доминанты как средство обеспечения мотивации школьников при обучении математике в основной школе

В статье рассматривается проблема обеспечения мотивации при обучении математике. Предложены средства, способствующие ее формированию, основными из которых являются задания на создание учебной доминанты в определенных содержательно-методических линиях курса алгебры и геометрии основной школы. Кратко представлены результаты апробации разработанных средств.

Ключевые слова: проблема мотивации при обучении математике, доминанта, задания на создание учебной доминанты, субъектный опыт.

АКТУАЛЬНОСТЬ

В настоящее время одной из значимых проблем обучения математики является поиск условий появления интереса у учащихся к математике, создания прочной мотивации к этому предмету. Это особенно трудно сделать в то время, когда внимание современных школьников удерживается не более восьми секунд, а математика требует сосредоточенности, абстрагирования от конкретных вещей. Одним из путей достижения указанных условий является обращение к субъектному опыту ребенка, в котором И. С. Якиманская выделяет четыре составляющих: эмоционально-ценностную, процессуальную, содержательную и коммуникативную. В процессе обучения менее всего обращаются к первой составляющей, хотя именно она отвечает за мотивацию. С одной стороны, она направлена на выделение человеком наиболее