

Пастухов Ю.Ф.¹ к.ф.-м.н., доцент кафедры технологий программирования

Пастухов Д.Ф.¹ к.ф.-м.н., доцент кафедры технологий программирования

Пастухов А.Ю.² магистрант

Чернов С.В.³ ведущий инженер

О СТРУКТУРЕ АЛГЕБРАИЧЕСКИХ ВЫЧЕТОВ И НЕВЫЧЕТОВ ОДИННАДЦАТОГО ПОРЯДКА В ПОЛЕ ВЫЧЕТОВ Z_p

¹Полоцкий государственный университет имени Евфросинии Полоцкой, Полоцк, Беларусь

² Витебский государственный университет имени П.М. Машерова, Витебск, Беларусь

³«Конструкторское бюро «Дисплей», Витебск, Беларусь

Аннотация.

Вычеты и невычеты одиннадцатого порядка в поле Z_p – элементы поля, для которых существует решение канонического уравнения одиннадцатой степени (с коэффициентом при старшем степени, равным единице), и свободным членом, равным заданному (фиксированному) элементу поля.

Структура вычетов одиннадцатого порядка выводится из критерия существования алгебраического уравнения степени n

Невычеты и вычеты одиннадцатой степени используются в алгебре, теории чисел, криптографии, компьютерной безопасности.

1. Введение.

В работе [3] исследовался вопрос о существовании решений алгебраических уравнений в кольце вычетов Z_m в результате – получено критерий (теорема 1) – условие существования(канонического) алгебраического уравнения степени n в кольце вычетов Z_m с образующими и свободным членом, взаимно простым с порядком кольца.

В этой работе представлена структура вычетов одиннадцатого порядка(степени) из более общего факта [3].

Например, из алгебры, известно, вычеты одиннадцатого порядка(степени) в поле Z_p – это такие элементы $a \in Z_p$, для которых существуют решения уравнения $x^{11} \equiv a \pmod{p}$, невычеты десятой степени(порядка) в поле Z_p – это такие элементы $a \in Z_p$, для которых нет решения уравнения $x^{11} \equiv a \pmod{p}$ Число образующих равно $\varphi(\varphi(m))$, где φ – мультипликативная функция Эйлера.

Из алгебры известно, что

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

Элементы кольца 0 и 1 всегда являются вычетами любой степени в кольце любого конечного порядка. естественным вопрос как устроены все вычеты, например, одиннадцатой степени?

Теорема 1. (Строение вычетов одиннадцатого порядка(степени) в поле Z_p)

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

1) $a = 0$ является вычетом одиннадцатой степени (так как существует тривиальное(очевидное) решение $x = 0$: $0^{11} = 0(\text{mod } p)$)

2) в случае все вычеты 11-ой степени имеют вид:

$$a_0 = 0, a_k = g^{\text{НОД}(p-1,11)*k} \quad k = 1, \overline{\frac{p-1}{\text{НОД}(p-1,11)}}$$

3) Количество вычетов равно в случае равно $\frac{p-1}{\text{НОД}(p-1,11)} + 1$ (прибавление 1 в формуле – это учет тривиального нулевого вычета)

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

Образующими кольца $Z_{p=7}$ являются элементы $\{3, 5\}$:

$$\{3^1 \equiv 3(\text{mod } 7), 3^2 \equiv 2(\text{mod } 7), 3^3 \equiv 6(\text{mod } 7), 3^4 \equiv 4(\text{mod } 7), 3^5 \equiv 5(\text{mod } 7), 3^6 \equiv 1(\text{mod } 7)\} \Rightarrow g = 3 - \text{образующий}$$

$$\{5^1 \equiv 5(\text{mod } 7), 5^2 \equiv 4(\text{mod } 7), 5^3 \equiv 6(\text{mod } 7), 5^4 \equiv 2(\text{mod } 7), 5^5 \equiv 3(\text{mod } 7), 5^6 \equiv 1(\text{mod } 7)\} \Rightarrow g = 5 - \text{образующий}$$

Рассмотрим, для примера, случай с образующий $g = 3$

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

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

По теореме 1 (критерию) вычеты $\frac{\text{НОД}(p-1,11)}{\text{НОД}(7-1,11)} = \frac{\text{НОД}(6,11)}{\text{НОД}(6,11)} = 1$

$$a_k = g^{\text{НОД}(p-1,11)*k} = g^{\text{НОД}(7-1,11)*k} = g^{1*k} \quad k = 1, \overline{\frac{p-1}{\text{НОД}(p-1,11)}} = 1, \overline{\frac{7-1}{\text{НОД}(7-1,11)}} = 1, \overline{\frac{7-1}{1}} = 1, 6$$

То есть вычеты, это: $a_{k=1} = g^{\text{НОД}(p-1,11)*k} = g^{1*1} = g^1 = 3^1 \equiv 3(\text{mod } 7)$

Также вычет, это: $a_{k=2} = g^{\text{НОД}(p-1,11)*k} = g^{1*2} = g^2 = 3^2 \equiv 2(\text{mod } 7)$

Также вычет, это: $a_{k=3} = g^{\text{НОД}(p-1,11)*k} = g^{1*3} = g^3 = 3^3 \equiv 6(\text{mod } 7)$

Также вычет, это: $a_{k=4} = g^{\text{НОД}(p-1,11)*k} = g^{1*4} = g^4 = 3^4 \equiv 4(\text{mod } 7)$

Также вычет, это: $a_{k=5} = g^{\text{НОД}(p-1,11)*k} = g^{1*5} = g^5 = 3^5 \equiv 5(\text{mod } 7)$

И еще вычет, это: $a_{k=6} = g^{\text{НОД}(p-1,11)*k} = g^{1*6} = g^6 = 3^6 \equiv 1(\text{mod } 7)$

Значит, вычеты – это 3, 2, 6, 4, 5, 1 ну, и, конечно, вычет 0 (пункт 1) теоремы 1).

Правильность сделанных выводов иллюстрирует строка вычислений:

$$\{0^{10} \equiv 0(\text{mod } 7), 1^{10} \equiv 1(\text{mod } 7), 2^{10} \equiv 2(\text{mod } 7), 3^{10} \equiv 4(\text{mod } 7), 4^{10} \equiv 4(\text{mod } 7), 5^{10} \equiv 2(\text{mod } 7), 6^{10} \equiv 1(\text{mod } 7)\}$$

Легко видеть, что все элементы поля Z_7 являются вычетами 11-ого порядка, невычетов 11-ого порядка-нет.

Список использованных источников:

1. Волосова Н.К., Волосов К.А., Волосова А.К., Пастухов Д.Ф., Пастухов Ю.Ф. Обобщение формулы Эйлера для непланарного графа. Москва, 2024.
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., 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.

4. 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.

5. 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.