если не все блоки данных доступны. В этом случае может потребоваться создание новых корректирующих символов для получения полного доступа к данным, что может повысить время доступа в случае неисправности.

Заключение

Система распределенного хранения данных на основе кодов Рида-Соломона - это мощный инструмент для хранения и обработки больших объемов данных на расстоянии. Она обеспечивает высокую производительность, масштабируемость и защиту данных в случае ошибок в передаче. Тем не менее, она также имеет свои недостатки, такие как высокая стоимость и сложность восстановления данных. В целом, использование системы распределенного хранения данных на основе кодов Рида-Соломона следует рассматривать в зависимости от конкретных потребностей организации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Y. Lin, X. Luo, Y. Li, J. Liu, and K. Li, "A Distributed Storage Architecture Based on Reed-Solomon Codes and Double Regenerating Codes," in 2013 International Conference on Cloud Computing and Big Data, 2013, pp. 249-253.
2. K. Shum, W. Chan, C. Lau, and S. Tse, "Distributed Storage System Based on Reed-Solomon Codes," in 2010 IEEE International Conference on Communications, 2010, pp. 1-5.
3. F. Qiu, H. Jin, X. Huo, and Y. Hu, "A Novel Distributed Storage System Based on Reed-Solomon Codes," in 2012 International Conference on Computing, Networking and Communications (ICNC), 2012, pp. 700-704.
4. L. R. Knudsen, "Reed-Solomon Codes and Their Applications," IEEE Communications Magazine, vol. 41, no. 8, pp. 70-76, Aug. 2003.

УДК 511 УДК 512 УДК 003.326

КРИТЕРИЙ, КОЛИЧЕСТВО И СТРУКТУРА КУБИЧЕСКИХ ВЫЧЕТОВ В ПОЛЕ Zp

Пастухов Юрий Феликсович[1], Пастухов Дмитрий Феликсович[1],
Волосов Константин Александрович[4], Чернов Сергей Васильевич[2] ,
Пастухов Александр Юрьевич [3] , Волосова Александра Константиновна [4],
Волосова Наталья Константиновна [5], Калинцев Сергей Викторович[1]
Полоцкий государственный университет имени Евфросинии Полоцкой, Полоцк, Беларусь
[2]«Конструкторское бюро «Дисплей», Витебск, Беларусь
[3] Витебский государственный университет имени П.М. Машерова, Витебск, Беларусь
[4]РУТ(МИИТ) Московский государственный университет путей сообщения Императора Николая II, Москва, Россия
[5]МГТУ им. Н.Э. Баумана, Москва, Россия

Аннотация

Кубические вычеты и невычеты в поле Z_p - элементы поля для которых существует решение канонического кубического уравнения с единичным коэффициентом при старшем члене и свободным членом, совпадающим с заданным элементом поля.

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

Кубические вычеты и невычеты используются в теории чисел, компьютерной безопасности криптографии.

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 теорема1 - 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 критерий кубических вычетов и невычетах из более общего критерия [1] существования решения канонического неоднородного алгебраического уравнения степени в кольцах, где мультипликативная группа порождается одним элементом(циклической). Так как мультипликативная группа поля Z_p Z_p^* состоит из всех ненулевых элементов и является циклической , так как р- 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 $x^2 \equiv a(\mathrm{mod}\,\mathrm{p})$, невычеты в поле Z_p - это такие элементы $a \in Z_p$, для которых не существуют решения уравнения $x^3 \equiv a(\mathrm{mod}\,\mathrm{p})$ Количество порождающих равно $\varphi(\varphi(\mathrm{m}))$, где $\varphi -$

функция Эйлера.

Известно, что

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

Теорема1 (Критерий , количество и структура кубических вычетов и невычетов в поле Zp)

Пусть Z_p – поле вычетов по простому модулю р. Пусть $g-$произвольный

образующий 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 $x=0$: $0^3 = 0(\mathrm{mod}\,\mathrm{p})$)

2) $a \neq 0$ пусть $a \neq 0 \Rightarrow a \in Z_p^* \Rightarrow \exists\, 1 \le \beta \le \varphi(\mathrm{p}) = \mathrm{p}-1$: $a = g^\beta \Leftrightarrow \beta = \log_g \mathrm{a}$ (1)

$a-$ кубический вычет в

$Z_p \Leftrightarrow \beta = \log_g a \equiv 0(\text{НОД}(\varphi(\mathrm{p}) = \mathrm{p}-1,\ \mathrm{n}=3)) \Leftrightarrow \beta$ *делится без остатка на* НОД(p−1, 3) (2)

$\text{НОД}(p-1,\,3) = \begin{cases} 3, \text{при}\ p = 3k+1(a) \\ 1, \text{при}\ p \neq 3k+1(b) \end{cases}$ (3) Условие (2) не зависит от выбора порождающего элемента. В случае (3b), очевидно, любой элемент является кубическим вычетом.

3) в случае (3a) все кубические вычеты имеют вид:

$a_0 = 0,\ a_k = g^{3k}\ \ k = \overline{1, \frac{p-1}{3}}$

4) Количество вычетов равно в случае (3а) равно *(p+2) /3*

Пример1 Рассмотрим для примера кольцо по простому модулю Z **,** количество образующих в Z_7 $\varphi(\varphi(\mathrm{m}=7)) = \varphi(6) = 2$, найдем их

Порождающие кольца это $\{3,5\}$:

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

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

Рассмотрим, например *образующий* $g=3$

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

По критерию(**теорема1**)

Ни 2, ни 5, ни 1 не делится на 3=*НОД(p-1=7-1=6,3)=3* следовательно 2, 3, 5 –невычеты.

$\log_{g=3}(a=1)=\beta=6 \Leftrightarrow 3^6 \equiv 1(\bmod 7)$ $\log_{g=3}(a=6)=\beta=3 \Leftrightarrow 3^3 \equiv 6(\bmod 7)$ По критерию(**теорема1**)

Так как 3 и 6 делится на 3 , следовательно 1, 6 –вычеты, ну и ,конечно, тривиальный вычет 0, который является вычетом произвольной степени в любом кольце.

Рассмотрим, например *образующий* $g=5$

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

По критерию(**теорема1**)

Ни 2, ни 5, ни 1 не делится на 3=*НОД(p-1=7-1=6,3)=3* следовательно 2, 3, 5 –невычеты.

$\log_{g=5}(a=1)=\beta=6 \Leftrightarrow 3^6 \equiv 1(\bmod 7)$ $\log_{g=5}(a=6)=\beta=3 \Leftrightarrow 3^3 \equiv 6(\bmod 7)$ По критерию(**теорема1**)

Так как 3 и 6 делится на 3 , следовательно 1, 6 –вычеты, ну и ,конечно, тривиальный вычет 0, который является вычетом произвольной степени в любом кольце.

Это действительно так- как показывает нижеследующая строка вычислений ниже:

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

Структура вычетов по пункту 4) теоремы 1 : 3 в 3-й степени(6) по модулю 7 и 3 в 6-й степени(1) по модулю7 , как и должно было быть на основании рассмотренного выше.

В то же время в Z_5 $\varphi(\varphi(m=5))=\varphi(4)=2$

Образующие кольца Z_5 это $\{2,3\}$:

$$\left\{2^1=2 \equiv 2(\bmod 5), 2^2=4 \equiv 4(\bmod 5), 2^3=8 \equiv 3(\bmod 5), 2^4=16 \equiv 1(\bmod 5)\right\} \Rightarrow g=2-\textit{образующий}$$

$$\left\{3^1=3 \equiv 3(\bmod 5), 3^2=9 \equiv 4(\bmod 5), 3^3=27 \equiv 2(\bmod 5), 3^4=81 \equiv 1(\bmod 5)\right\} \Rightarrow g=3-\textit{образующий}$$

НОД(p-1=5-1=4,3)=1 – на 1 делится любое натуральное число, поэтому все элементы в Z_5 - кубические вычеты :

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

Таким образом, структура в отличие от квадратичных вычетов, структура кубических вычетов зависит от простого числа p – точнее от остатка его деления на 3.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. 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 Пастухов Ю.Ф., Пастухов Д.Ф., Чернов С.В., Волосова Н.К., Волосов К.А., Волосова А.К. Тенденции развития науки и образования. 2023. № 101-4. С. 114-117.