11 ноября 2021

Задание циклического кода идемпотентом.

$C \subset \mathbb{F}_p^n \cong \mathbb{F}_p[x] / (x^n - 1)$

C — циклический $\Leftrightarrow$ $f \in \mathbb{F}_p[x]$, $f \mid (x^n - 1)$ в $\mathbb{F}_p$

$C_f = \{ h(x) f(x) \bmod (x^n - 1) \} =$

$x^n - 1 = f(x) g(x)$

$= \{ h(x) f(x), \; h(x) \bmod g(x) \}$

Условие: $\boxed{\text{НОД}(p, n) = 1}$

$(x^n - 1)' = n x^{n-1} \Rightarrow$

$\text{НОД}(x^n - 1, n x^{n-1}) = 1 \Rightarrow$ у $x^n - 1$ нет кратных корней в полях типа $\mathbb{F}_{p^m}$.

нет кратных корней

$x^n - 1 = f(x) g(x) \Rightarrow \text{НОД}(f(x), g(x)) = 1.$

корней

Теорема Безу $\Rightarrow \exists\, a(x), b(x) \in \mathbb{F}_p[x]$

$a(x) f(x) + b(x) g(x) = 1.$

Рассмотрим $e(x) \bmod x^n - 1$

$e(x) = a(x) f(x) \in \mathbb{F}_p[x] / x^n - 1$

1) $e(x) = e(x) \cdot 1 = e(e + b \cdot g) = e^2 + a \cdot f \cdot b \cdot g \equiv$

$e^2 \bmod x^n - 1$

$$\boxed{e^2(x) = e(x) \bmod x^n - 1} \quad !$$

$e(x)$ – идемпотент кольца $\mathbb{F}_p[x] / x^n - 1$

2) $f(x) = f(x) \cdot 1 = f(e(x) + b(x) \cdot g(x)) = f \cdot e \bmod x^n - 1$

$$\boxed{f \cdot e \equiv f \bmod x^n - 1} \Rightarrow$$

$e(x)$ делит $f(x)$ в кольце $\mathbb{F}_p[x] / x^n - 1$!

$e(x) = q(x) \cdot f(x) \Rightarrow \deg e(x) \geq \deg f(x)$!

$f(x)$ это многочлен минимальной степени в коде C_f, но мы нашли другую образующую данной степени !

Проверим: $\boxed{C_f = C_e}$

Д-во: $h(x) f(x) = \big(h(x) f(x)\big) e(x) \mod x^n - 1$

$\Rightarrow C_f \subset C_e$

$e(x) = a(x) f(x) \Rightarrow h(x) e(x) = h(x) a(x) f(x) \in C_f$

$C_e \subset C_f$ ☞

Мы нашли новую образующую идеала C_f : $af + bg = 1 \Rightarrow$

$e = af \mod x^n - 1$ – другая образующая.

Второе описание циклического кода C_f.

$$B_e = \left\{ m \in {}^{\mathbb{F}_p[x]}/_{(x^n-1)} : m(x) e(x) \equiv m(x) \right\} \quad (*)$$

Лемма $\boxed{C_f = B_e}$.

Д-во: $fe \equiv f \mod x^n - 1 \Rightarrow f \in B_e$

$h \cdot f \in C_f \quad (h \cdot f) \cdot e \equiv h(f \cdot e) = hf \Rightarrow$

$C_f \subset B_e$.

Пусть $m_e \equiv m \mod x^n - 1$

$m \cdot af = (mq) f \in C_f \Rightarrow$

$B_e \subset C_f$. ▨

Следствие Идемпотент e однозначно определяется с-вом (*).

Д-во: $C_f = B_e = B_{e'} \Rightarrow$

$e' \in B_{e'} = B_e \Rightarrow e' \cdot e \equiv e \mod x^n - 1$

$(e')^2 \equiv e$ ‖ ‖

$e \in B_e = B_{e'} \Rightarrow e \cdot e' = e' \mod x^n - 1$

Вывод: $e \equiv e' \mod x^n - 1$.

Вопрос: $e \in C_f$ это единственный идемпотент в C_f?

Как мы нашли e?

$x^n - 1 = f \cdot g \Rightarrow af + bg = 1 \Rightarrow$

$e = af$ — идемпотент в $\mathbb{F}_p[x]/(x^n - 1)$

$x^n - 1 = \underbrace{(f \cdot f_1)}_{\text{взаимно просты}} \cdot g_1 \Rightarrow (a_1 f_1) f + b_1 g_1 = 1$

$e_1(x) = a_1 f_1 f_-$ — идемпотент в C_f

Выводы: $x^n - 1 = f \cdot g \Rightarrow$

$\exists\, a, b \in \mathbb{F}_p[x] \quad a \cdot f + b g = 1 \Rightarrow$

$e = a \cdot f \in \mathbb{F}_p[x] \quad e^2 \equiv e \mod x^n - 1.$

$C_f = C_e = B_e = \{ m \in \mathbb{F}_p[x]/_{x^n-1} \mid me = e \}$

ВОПРОС: Можно ли восстановить f по e?

$e = a \cdot f$, где $af + bg = 1$.

В частности, $НОД(a, g) = 1 \Rightarrow$

$НОД(e(x), x^n - 1) = НОД(af, f \cdot g) =$

$= f \cdot НОД(a, g) = \boxed{f = НОД(e, x^n - 1)}$

С-ва элемент $e(x) \bmod x^n - 1$.

1) $e^2 = e \Rightarrow (1-e)^2 = 1 - 2e + e^2 = 1 - e$

$\Downarrow$

$(1-e)^2 = 1 - e$

2) $e(x)^2 \equiv e(x) \bmod (x^n - 1) \iff$

$e(x)(e(x)-1) \equiv 0 \bmod (x^n - 1)$

содержит все корни из 1 степени n!

Напоминание: примитивный корень степени n из 1.

$d = \operatorname{ord}^{\times}_{\text{mod } n} p = \operatorname{ord}_{(\mathbb{Z}/n\mathbb{Z})^{\times}} p \Rightarrow$

$\mathbb{F}_p^{\times} \; d = p^d - 1 \equiv 0 \bmod n \Rightarrow$

$\mathbb{F}_{p^d}^{\times}$ содержит элемент d порядка n.

$e(x) \cdot (e(x)-1) \equiv 0 \bmod (x^n - 1)$

содержит в себе все корни степени n из 1.

$f(x) \cdot g(x) = x^n - 1.$

$f(x) = \text{нод}(e(x), x^n - 1)$

$g(x) = \text{нод}(e(x) - 1, x^n - 1)$.

Упражнение $f \cdot g = x^n - 1$

$C_f^{-1} = C_{\tilde{g}} \overset{?}{=}$ в $\widetilde{e(x)-1}$

$\tilde{g}(x) = x^{\deg g} g\left(\frac{1}{x}\right)$

Проблема Обычно, нам известны корни делителей многочлена $x^n - 1$:

Каждый делитель $\overset{1:1}{\longleftrightarrow}$ циклотомическая орбита α

$\alpha \in \mathbb{F}_{p^d}$!!

Как найти коэффициенты многочлена f

Ответ 1 PARI — калькулятор по теории чисел.

$x^{27} - 1 \in \mathbb{F}_2[x] \overset{\text{PARI}}{\Rightarrow}$ разложение.

Ответ 2 Пример. (Ниже)

$$x^{23} - 1 \in \mathbb{F}_2[x]$$

Циклотомические орбиты mod 23

n	1	2	3	4	5	6	7	8	9	10	11	mod 23
2^n	2	4	8	16	9	18	13	3	6	12	1	

$$\mathrm{ord}^{\times}_{\mathrm{mod}\,23} 2 = 11 \Rightarrow \text{Получаем}$$

Неприводимый делитель $x^{23}-1$

$$f(x) = \prod_{k=1}^{11} \left(x - \alpha^{2^k} \right) \in \mathbb{F}_2[x]$$

α – примитивный корень порядка 23 над $\mathbb{F}_2$

$$\alpha \in \mathbb{F}_{2^{11}} = \mathbb{F}_{2048}$$

Выводы! Имеются две циклотомические орбиты:

$$\mathbb{Z}_{23}^{\times} = \{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18 \bmod 23\}$$

$R_- = -R_+ = \{5, 7, \dots\}$ (9)

Следовательно: имеется только два неприводимых множителя степени 11 над $\mathbb{F}_2$

$$x^{23} - 1 = (x-1) \underbrace{f}_{=} \cdot \underbrace{g}_{=} \qquad \deg f = \deg g = 11$$

f и g зависят от выбора α

$$f(x) = \prod_{k \in R_+} (x - \alpha^k)$$

$$g(x) = \prod_{k \in R_-} (x - \alpha^k)$$

Видим корни в $\mathbb{F}_{2^{11}}$.

Пусть $d(C_f)$ – минимальный ненулевой вес циклического кода C_f.

По Теореме:

$$d(C_f) \geq 5 \qquad R_+ = \{\underbrace{1, 2, 3, 4}_{\text{4 степени подряд}}, 6. \}$$

$$C_f = C_g = [23, 23-11, d] \qquad d \geq 5.$$

$23 - 11 = 12$

Идея: Использовать идемпотенты для нахождения f и g.

Рассмотрим многочлен

$$e_+(x) = \sum_{k \in R_+} x^k \in \mathbb{F}_2[x]$$

$$= x^1 + x^2 + x^3 + x^4 + x^6 + x^8 + x^9 + x^{12} + x^{13} + x^{16} + x^{18}$$

$$e_+(x)^2 \equiv \left(\sum_{k \in R_+} x^k\right)^2 =$$

$\mod x^{23} - 1$ т.е. $x^{23} = 1$

$$= \sum_{k \in R_+} x^{2k} \equiv \sum_{k \in R_+} x^k \equiv e(x) \mod x^{23} - 1$$

$k \in R_+$ – циклотомическая область по модулю 23

Мы нашли идемпотент в кольце

$$A_{23}^{(2)} = \mathbb{F}_2[x] / x^{23} - 1.$$

$$B_e = \{ m \in A_{23}^{(2)} : me = m \} =$$

$$C_{t,2l}$$

$$f = \mathrm{HOД}(e(x), x^{23} - 1) \Rightarrow$$

Не надо считать в поле $\mathbb{F}_{2^{11}}$

алгоритм Евклида над $\mathbb{F}_2$.

Мы нашли неприводимый многочлен степени 11

Следующая тема: Понять и обобщить идею разложения $X^{23}-1$, используя квадратичные вычеты и невычеты (арифметика!)