

Часть I

Конечные поля или поля Галуа.

II

Разделы

- 1 Поля вычетов по модулю простого числа
- 2 Вычисление элементов в конечных полях
- 3 Линейная алгебра над конечным полем
- 4 Корни многочленов над конечным полем
- 5 Существование и единственность поля Галуа из p^n элементов
- 6 Циклические подпространства
- 7 Задачи с решениями
- 8 Что надо знать

Разделы

- 1 Поля вычетов по модулю простого числа
- 2 Вычисление элементов в конечных полях**
- 3 Линейная алгебра над конечным полем
- 4 Корни многочленов над конечным полем
- 5 Существование и единственность поля Галуа из p^n элементов
- 6 Циклические подпространства
- 7 Задачи с решениями
- 8 Что надо знать

Разделы

- 1 Поля вычетов по модулю простого числа
- 2 Вычисление элементов в конечных полях
- 3 Линейная алгебра над конечным полем**
- 4 Корни многочленов над конечным полем
- 5 Существование и единственность поля Галуа из p^n элементов
- 6 Циклические подпространства
- 7 Задачи с решениями
- 8 Что надо знать

Разделы

- 1 Поля вычетов по модулю простого числа
- 2 Вычисление элементов в конечных полях
- 3 Линейная алгебра над конечным полем
- 4 Корни многочленов над конечным полем**
- 5 Существование и единственность поля Галуа из p^n элементов
- 6 Циклические подпространства
- 7 Задачи с решениями
- 8 Что надо знать

Разделы

- 1 Поля вычетов по модулю простого числа
- 2 Вычисление элементов в конечных полях
- 3 Линейная алгебра над конечным полем
- 4 Корни многочленов над конечным полем
- 5 Существование и единственность поля Галуа из p^n элементов**
- 6 Циклические подпространства
- 7 Задачи с решениями
- 8 Что надо знать

Вычисления в мультипликативной группе расширения поля

Начнём с примера поля \mathbb{F}_2^4 .

Пример

Поле \mathbb{F}_2^4 можно строить с помощью любого из трех неприводимых над \mathbb{F}_2 многочленов (но пока не доказано):

$$x^4 + x + 1, \quad x^4 + x^3 + 1, \quad x^4 + x^3 + x^2 + x + 1$$

Сделаем это, взяв многочлен $f(x) = x^4 + x + 1$.

Вычисления в мультипликативной группе расширения поля

Начнём с примера поля \mathbb{F}_2^4 .

Пример

Поле \mathbb{F}_2^4 можно строить с помощью любого из трех неприводимых над \mathbb{F}_2 многочленов (но пока не доказано):

$$x^4 + x + 1, \quad x^4 + x^3 + 1, \quad x^4 + x^3 + x^2 + x + 1$$

Сделаем это, взяв многочлен $f(x) = x^4 + x + 1$.

Будем задавать элементы \mathbb{F}_2^4 наборами коэффициентов многочлена-остатка при делении на f , записывая их в порядке **возрастания** степеней.

Порождающим является элемент $\alpha = x$, который записывается как $(0, 1, 0, 0)$.

Вычислим степени α , сведя результаты в таблицу.

Мультипликативная группа поля $\mathbb{F}_2^4 \cong \mathbb{F}_2[x]/(x^4 + x + 1)$

$\alpha^4 = \alpha + 1$	степень α	1	x	x^2	x^3
	$\alpha =$	(0,	1,	0,	0)
	$\alpha^2 =$	(0,	0,	1,	0)
	$\alpha^3 =$	(0,	0,	0,	1)
	$1 + \alpha = \alpha^4 =$	(1,	1,	0,	0)
	$\alpha + \alpha^2 = \alpha^5 =$	(0,	1,	1,	0)
	$\alpha^2 + \alpha^3 = \alpha^6 =$	(0,	0,	1,	1)
	$\alpha^3 + \alpha + 1 = \alpha^3 + \alpha^4 = \alpha^7 =$	(1,	1,	0,	1)
	$1 + \alpha^2 = \alpha + 1 + \alpha^2 + \alpha = \alpha^8 =$	(1,	0,	1,	0)
	$\alpha + \alpha^3 = \alpha^9 =$	(0,	1,	0,	1)
	$\alpha^2 + 1 + \alpha = \alpha^2 + \alpha^4 = \alpha^{10} =$	(1,	1,	1,	0)
	$\alpha + \alpha^2 + \alpha^3 = \alpha^{11} =$	(0,	1,	1,	1)
	$1 + \alpha + \alpha^2 + \alpha^3 = \alpha^2 + \alpha^3 + \alpha^4 = \alpha^{12} =$	(1,	1,	1,	1)
	$1 + \alpha^2 + \alpha^3 = \alpha + \alpha^2 + \alpha^3 + \alpha^4 = \alpha^{13} =$	(1,	0,	1,	1)
	$1 + \alpha^3 = \alpha + \alpha^3 + \alpha^4 = \alpha^{14} =$	(1,	0,	0,	1)
	$1 = \alpha + \alpha^4 = \alpha^{15} =$	(1,	0,	0,	0)

Мультипликативная группа поля $\mathbb{F}_2^4 \cong \mathbb{F}_2[x]/(x^4 + x + 1) \dots$

Имея такую таблицу, очень просто производить умножение.

Пример: $(x^3 + x + 1) \cdot (x^2 + x + 1) = ?$

Мультипликативная группа поля $\mathbb{F}_2^4 \cong \mathbb{F}_2[x]/(x^4 + x + 1) \dots$

Имея такую таблицу, очень просто производить умножение.

Пример: $(x^3 + x + 1) \cdot (x^2 + x + 1) = ?$

- 1 Перемножить, учитывая $x^4 = x + 1$ — можно, но сложно...

Мультипликативная группа поля $\mathbb{F}_2^4 \cong \mathbb{F}_2[x]/(x^4 + x + 1) \dots$

Имея такую таблицу, очень просто производить умножение.

Пример: $(x^3 + x + 1) \cdot (x^2 + x + 1) = ?$

- 1 Перемножить, учитывая $x^4 = x + 1$ — можно, но сложно...
- 2 С помощью таблицы:
 - представляем многочлены в векторной форме и по ней — в виде степеней $\alpha = x$:

$$x^3 + x + 1 \leftrightarrow (1, 1, 0, 1) \leftrightarrow \alpha^7,$$

$$x^2 + x + 1 \leftrightarrow (1, 1, 1, 0) \leftrightarrow \alpha^{10}$$

- перемножая, получаем: $\alpha^7 \alpha^{10} = \alpha^{17} = \alpha^2 = x^2$.

Таким образом: $(x^3 + x + 1) \cdot (x^2 + x + 1) = x^2$.

Пути доказательства

Теперь можно вернуться к вопросу о существовании

- а) конечного поля \mathbb{F}_q размера q , показав, что всегда $q = p^n$;
- б) неприводимого многочлена степени n над \mathbb{F}_p

(везде p — простое, n — натуральное).

Пути доказательства

Теперь можно вернуться к вопросу о существовании

- а) конечного поля \mathbb{F}_q размера q , показав, что всегда $q = p^n$;
- б) неприводимого многочлена степени n над \mathbb{F}_p
(везде p — простое, n — натуральное).

Это можно сделать двумя способами.

- а) \Rightarrow б) доказать существование поля из p^n элементов, откуда вывести существование неприводимого многочлена степени n над \mathbb{F}_p ;
- б) \Rightarrow а) установить существование неприводимого многочлена f степени n над \mathbb{F}_p , откуда уже следует существование поля из p^n как факторкольца по идеалу (f) .

Мы пойдём **вторым** путём.

Существование неприводимого многочлена

Докажем существование **нормированного неприводимого многочлена** в полях Галуа.

Для таких многочленов выполняется аналог основной теоремы арифметики: *каждый нормированный многочлен однозначно разлагается на произведение степеней неприводимых многочленов.*

Существование неприводимого многочлена

Докажем существование **нормированного неприводимого многочлена** в полях Галуа.

Для таких многочленов выполняется аналог основной теоремы арифметики: **каждый нормированный многочлен однозначно разлагается на произведение степеней неприводимых многочленов.**

Действительно:

- разложение в евклидовом кольце **однозначно** (с точностью до умножения на обратимые элементы — делители);
- в случае кольца многочленов над полем обратимые элементы — ненулевые константы (многочлены степени 0);
- выбор старшего коэффициента 1 однозначно определяет сомножители.

Количество неприводимых нормированных многочленов

Лемма (о числе d_n)

Если d_n — число неприводимых нормированных многочленов степени n над \mathbb{F}_p , то

$$\sum_{m|n} m \cdot d_m = p^n.$$

Количество неприводимых нормированных многочленов

Лемма (о числе d_n)

Если d_n — число неприводимых нормированных многочленов степени n над \mathbb{F}_p , то

$$\sum_{m|n} m \cdot d_m = p^n.$$

Доказательство

Занумеруем $i = 1, \dots, d_n$ все неприводимые нормированные многочлены степени n и сопоставим им формальную переменную $f_{i,n} \Rightarrow$ произвольному такому многочлену однозначно сопоставлен моном (многочлен степени n_j берётся в степени s_j):

$$f_{i_1, n_1}^{s_1} \cdot \dots \cdot f_{i_r, n_r}^{s_r}, \quad \text{причем} \quad \sum_{j=1}^r n_j s_j = n.$$

Количество неприводимых нормированных многочленов...

Доказательство (продолжение)

Поэтому все нормированные многочлены перечисляются формальным бесконечным произведением

$$\prod_{i,n} \left(\sum_{k=0}^{\infty} f_{i,n}^k \right) = \sum f_{i_1, n_1}^{s_1} \cdot \dots \cdot f_{i_r, n_r}^{s_r} \quad (*)$$

(раскрыты скобки и бесконечное произведение записано в виде формального ряда).

Сделаем замену переменных $f_{i,n} = t^n$, которая делает **все многочлены одной степени неразличимыми**.

Количество неприводимых нормированных многочленов...

Доказательство (продолжение)

$$\prod_{i,n} \left(\sum_{k=0}^{\infty} f_{i,n}^k \right) = \sum f_{i_1, n_1}^{s_1} \cdot \dots \cdot f_{i_r, n_r}^{s_r} \quad (*)$$

Приведение подобных приведёт к тому, что:

в **правой части** (*) будет ряд от переменной t .

Коэффициент при t^n в этом ряде равен числу нормированных многочленов степени n , т.е. p^n :

$$\sum_{n=0}^{\infty} p^n t^n.$$

Количество неприводимых нормированных многочленов...

Доказательство (продолжение)

$$\prod_{i,n} \left(\sum_{k=0}^{\infty} f_{i,n}^k \right) = \sum_{n=0}^{\infty} p^n t^n \quad (*)$$

В **левой части** все неприводимые многочлены степени n дадут одинаковый множитель (сумму бесконечной геометрической прогрессии со знаменателем t^n) и $(*)$ превращается в

$$\prod_n \left(\sum_{k=0}^{\infty} t^{nk} \right)^{d_n} = \sum_{n=0}^{\infty} p^n t^n.$$

Количество неприводимых нормированных многочленов...

Доказательство (продолжение)

По формуле *суммы бесконечной геометрической прогрессии*:

$$\prod_n \frac{1}{(1 - t^n)^{d_n}} = \frac{1}{1 - pt}.$$

Прологарифмируем («-» в обеих частях равенства сокращаются, $n \mapsto m$):

$$\sum_m d_m \ln(1 - t^m) = \ln(1 - pt).$$

Продифференцируем по t («-» в обеих частях равенства сокращаются):

$$\sum_m d_m \frac{mt^{m-1}}{1 - t^m} = \frac{p}{1 - pt}.$$

Количество неприводимых нормированных многочленов...

Доказательство (продолжение) $\left(\sum_n d_n \frac{nt^{n-1}}{1-t^n} = \frac{p}{1-pt} \right)$

Снова воспользуемся формулой суммой геометрической прогрессии:

$$\sum_{m,k} d_m m t^{m-1} t^{mk} = \sum_n p^{n+1} t^n.$$

Умножаем на t обе части равенства:

$$\sum_{m,k} m d_m t^{m(k+1)} = \sum_n p^n t^n.$$

Равенство коэффициентов при одинаковых степенях t и есть утверждение леммы $\left(\sum_{m|n} m \cdot d_m = p^n \right)$.

Важные замечания

1. Существование неприводимых многочленов

Из данной леммы следует неравенство $nd_n \leq p^n$. Простая оценка

$$nd_n = p^n - \sum_{k|n, k < n} kd_k \geq p^n - \sum_{k=0}^{n-1} p^k = p^n - \frac{p^n - 1}{p - 1} > 0.$$

доказывает, что $d_n > 0$, а это означает, что существует **хотя бы один** неприводимый многочлен степени n .

Важные замечания

1. Существование неприводимых многочленов

Из данной леммы следует неравенство $nd_n \leq p^n$. Простая оценка

$$nd_n = p^n - \sum_{k|n, k < n} kd_k \geq p^n - \sum_{k=0}^{n-1} p^k = p^n - \frac{p^n - 1}{p - 1} > 0.$$

доказывает, что $d_n > 0$, а это означает, что существует **хотя бы один** неприводимый многочлен степени n .

2. Среднее число неприводимых нормированных многочленов

Из данной леммы вытекает, что при $n \rightarrow \infty$ имеем $d_n \sim p^n/n$. Т.е. **неприводимые нормированные** многочлены составляют приблизительно $1/n$ -ю часть всех многочленов степени n над полем \mathbb{F}_p .

Изоморфизм полей Галуа с одинаковым числом элементов

Докажем вторую часть основной теоремы о конечных полях:
любые два поля с одинаковым числом элементов изоморфны.

Теорема

Пусть m — минимальный многочлен элемента $\alpha \in \mathbb{F}_p^n$ и d — её степень.

Тогда поле $\mathbb{F}_p[x]/(m)$ изоморфно подполю \mathbb{F}_p^d , порожденному степенями α .

Изоморфизм полей Галуа с одинаковым числом элементов

Докажем вторую часть основной теоремы о конечных полях:
любые два поля с одинаковым числом элементов изоморфны.

Теорема

Пусть m — минимальный многочлен элемента $\alpha \in \mathbb{F}_p^n$ и d — её степень.

Тогда поле $\mathbb{F}_p[x]/(m)$ изоморфно подполю \mathbb{F}_p^d , порожденному степенями α .

Доказательство

Степени α принадлежат d -мерному пространству с базисом $1, \alpha, \alpha^2, \dots, \alpha^{d-1}$, которое является подполем поля \mathbb{F}_p^n , поскольку замкнуто относительно сложения и умножения и содержит 0 и 1 .

Разделы

- 1 Поля вычетов по модулю простого числа
- 2 Вычисление элементов в конечных полях
- 3 Линейная алгебра над конечным полем
- 4 Корни многочленов над конечным полем
- 5 Существование и единственность поля Галуа из p^n элементов
- 6 Циклические подпространства**
- 7 Задачи с решениями
- 8 Что надо знать

Кольцо $\mathbb{F}_p[x]/(f)$

В приложениях часто используется кольцо многочленов $K(p, f) = \mathbb{F}_p[x]/(f)$ по модулю главного идеала (f) **возможно приводимого** многочлена $f \in \mathbb{F}_p[x]$.

Если f неприводим, то $K(p, f)$ — поле и этот случай уже рассмотрен.

Кольцо $\mathbb{F}_p[x]/(f)$

В приложениях часто используется кольцо многочленов $K(p, f) = \mathbb{F}_p[x]/(f)$ по модулю главного идеала (f) **ВОЗМОЖНО ПРИВОДИМОГО** многочлена $f \in \mathbb{F}_p[x]$.

Если f неприводим, то $K(p, f)$ — поле и этот случай уже рассмотрен.

В любом случае $K(p, f)$ — векторное пространство над \mathbb{F}_p т.е. совокупность многочленов степени меньшей $\deg f$.

$$\mathbb{F}_p[x] = \{0, 1, \dots, p-1, x, x+1, \dots, f, \dots\};$$

$$(f) = \bar{f} = \{t \cdot f\}, \quad t \in \mathbb{F}_p[x];$$

$$\mathbb{F}_p[x]/(f) = \{\bar{f}, \bar{g}, \bar{h}, \dots\}, \quad \deg \bar{f}, \deg \bar{g}, \dots \leq \deg f - 1;$$

$$\bar{g} = \{t \cdot f + g\}; \quad \bar{h} = \{t \cdot f + h\};$$

...

$$\bar{g} + \bar{f} = \bar{g}, \quad \bar{g} \cdot \bar{f} = \bar{f}.$$

Нормированный делитель порождающего элемента идеала

Теорема

Пусть φ — *неприводимый нормированный многочлен*, который делит f . Тогда

- 1 совокупность всех вычетов, кратных φ , образует идеал в кольце классов вычетов по модулю f :

$$I_\varphi \stackrel{\text{def}}{=} \{t \cdot \varphi\} \triangleleft \mathbb{F}_p[x]/(f).$$

- 2 φ — *единственный в I_φ нормированный многочлен минимальной степени*.

Нормированный делитель порождающего элемента идеала

Теорема

Пусть φ — *неприводимый нормированный многочлен*, который делит f . Тогда

- 1 совокупность всех вычетов, кратных φ , образует идеал в кольце классов вычетов по модулю f :

$$I_\varphi \stackrel{\text{def}}{=} \{t \cdot \varphi\} \triangleleft \mathbb{F}_p[x]/(f).$$

- 2 φ — *единственный в I_φ нормированный многочлен минимальной степени*.

Доказательство

$$u, v, \varphi \in \mathbb{F}_p[x], \quad k = \deg \varphi \leq \deg f$$

$$\varphi = a_0 + a_1x + \dots + a_{k-1}x^{k-1} + x^k, \quad f = \psi\varphi.$$

Нормированный делитель...

1. Проверим, что I_φ — идеал в кольце $\mathbb{F}_p[x]/(f)$.

1

$$\left\{ \begin{array}{l} \bar{g} \in I_\varphi \\ \bar{h} \in \mathbb{F}_p[x]/(f), \bar{h} \subseteq \bar{g} \end{array} \right. \Leftrightarrow \left\{ \begin{array}{l} \bar{g} = u\varphi \\ \bar{h} = v\varphi = vu\varphi \end{array} \right. \Rightarrow \bar{h} \in I_\varphi.$$

2

$$\bar{g}, \bar{h} \in I_\varphi \Leftrightarrow \left\{ \begin{array}{l} \bar{g} = u\varphi \\ \bar{h} = v\varphi \end{array} \right. \Rightarrow \bar{g} + \bar{h} = (u + v)\varphi \in I_\varphi.$$

Нормированный делитель...

2. Покажем, что в I_φ нет других, кроме

$$\varphi = a_0 + a_1x + \dots + a_{k-1}x^{k-1} + x^k$$

нормированных многочленов степени, меньшей $k = \deg \varphi$.

Пусть

$$g = b_0 + b_1x + \dots + x^m.$$

Тогда:

$$\bar{g} \in I_\varphi \Leftrightarrow g = u\varphi \Rightarrow \deg g = m \geq \deg \varphi = k.$$

Подыдеал как векторное пространство

Теорема

Пусть φ — неприводимый нормированный делитель многочлена $f \in \mathbb{F}_p[x]$ отличный от f , $\deg f = n$, $\deg \varphi = k$. Тогда идеал (φ) — векторное пространство размерности $n - k$.

Подыдеал как векторное пространство

Теорема

Пусть φ — неприводимый нормированный делитель многочлена $f \in \mathbb{F}_p[x]$ отличный от f , $\deg f = n$, $\deg \varphi = k$. Тогда идеал (φ) — векторное пространство размерности $n - k$.

Доказательство

Без доказательства.

Циклическое пространство: определение

- Пусть V — n -мерное векторное пространство над некоторым полем F .
- Фиксируем некоторый базис V .
- Тогда $V \cong F^n = \{ (a_0, \dots, a_{n-1}) \mid a_i \in F, i = 0, 1, \dots, n-1 \}$ — координатное пространство.

Определение

Подпространство координатного пространства F^n называется *циклическим*, если вместе с набором (a_0, \dots, a_{n-1}) оно содержит циклический сдвиг (вправо) этого набора, т.е. набор $(a_{n-1}, a_0, \dots, a_{n-2})$ (а следовательно и все циклические сдвиги на произвольное число позиций влево и вправо).

Кольцо классов вычетов по модулю многочлена $x^n - 1$

В кольце $\mathbb{F}_p[x]/(x^n - 1)$, рассматриваемом как векторное пространство над полем \mathbb{F}_p имеется базис $\{ \bar{1}, \bar{x}, \dots, \overline{x^{n-1}} \}$.

Циклический сдвиг координат в этом базисе равносильно умножению на x :

$$\begin{aligned} \overline{(a_0 + a_1x + \dots + a_{n-2}x^{n-2} + a_{n-1}x^{n-1})} \cdot \bar{x} &= \\ &= \overline{(a_0x + a_1x^2 + \dots + a_{n-2}x^{n-1} + a_{n-1}x^n)} = \\ &= \overline{(a_{n-1} + a_0x + a_1x^2 + \dots + a_{n-2}x^{n-1})}, \end{aligned}$$

т.к. в этом кольце $x^n = 1$.

Идеал в $\mathbb{F}_p[x]/(x^n - 1)$ — циклическое пространство

Теорема

Пусть I — подпространство кольца $\mathbb{F}_p[x]/(x^n - 1)$.

Тогда I — *циклическое* $\Leftrightarrow I \triangleleft \mathbb{F}_p[x]/(x^n - 1)$.

Идеал в $\mathbb{F}_p[x]/(x^n - 1)$ — циклическое пространство

Теорема

Пусть I — подпространство кольца $\mathbb{F}_p[x]/(x^n - 1)$.

Тогда I — **циклическое** $\Leftrightarrow I \triangleleft \mathbb{F}_p[x]/(x^n - 1)$.

Доказательство

- Если подпространство I — **идеал**, то оно замкнуто относительно умножения на \bar{x} , а это умножение и есть циклический сдвиг $\Rightarrow I$ — **циклическое**.

Идеал в $\mathbb{F}_p[x]/(x^n - 1)$ — циклическое пространство

Теорема

Пусть I — подпространство кольца $\mathbb{F}_p[x]/(x^n - 1)$.

Тогда I — **циклическое** $\Leftrightarrow I \triangleleft \mathbb{F}_p/(x^n - 1)$.

Доказательство

- Если подпространство I — **идеал**, то оно замкнуто относительно умножения на \bar{x} , а это умножение и есть циклический сдвиг $\Rightarrow I$ — **циклическое**.
- Пусть I — **циклическое подпространство** кольца $\mathbb{F}_p/(x^n - 1)$ и $g \in I$.
Тогда $g \cdot \bar{x}, g \cdot \bar{x}^2, \dots$ — циклические сдвиги, т.е. также принадлежат I .
Значит, $g \cdot \bar{f} \in I$ для любого многочлена f , поэтому I — **идеал**.

Примитивные корни

Было показано: *любой многочлен с коэффициентами из \mathbb{F}_p разлагается на линейные множители в некотором поле*

$\mathbb{F}_q = \mathbb{F}_p^n$ *характеристики p .*

Пусть \mathbb{F}_q — поле характеристики p , в котором разлагается многочлен $x^n - 1$.

Примитивные корни

Было показано: *любой многочлен с коэффициентами из \mathbb{F}_p разлагается на линейные множители в некотором поле*

$\mathbb{F}_q = \mathbb{F}_p^n$ *характеристики p .*

Пусть \mathbb{F}_q — поле характеристики p , в котором разлагается многочлен $x^n - 1$. Справедливо:

- В \mathbb{F}_q выполняется равенство $x^{kp} - 1 = (x^k - 1)^p$, поэтому интересен случай, когда n взаимно просто с p : тогда у многочлена $x^n - 1$ **кратных** корней нет (он взаимно прост со своей производной nx^{n-1}).
- Равенство $x^n = 1$ означает, что порядок элемента x в мультипликативной циклической группе \mathbb{F}_q^* делит n .

Вывод: корни уравнения $x^n - 1 = 0$ образуют *группу корней степени n из единицы* — **подгруппу** в \mathbb{F}_q^* .

Эта подгруппа также циклическая; её порождающие элементы называются *примитивными корнями степени n* .

Количество и степени неприводимых делителей $x^n - 1$

Подгруппа в циклической группе существует iff её порядок делит порядок циклической группы \Rightarrow

Количество и степени неприводимых делителей $x^n - 1$

Подгруппа в циклической группе существует iff её порядок делит порядок циклической группы \Rightarrow поле \mathbb{F}_q содержит группу корней из единицы степени n iff $n \mid (q - 1)$.

Чтобы вернуться от разложения $x^n - 1$ на **линейные** множители в поле $\mathbb{F}_q = \mathbb{F}_p^n$ (корни из 1) к разложению на **неприводимые** множители в поле \mathbb{F}_p , нужно понять, **какие корни из единицы будут входить в неприводимый делитель $f(x)$** .

Если β — корень $f(x)$, то β^p, β^{p^2} и т.д. — также его корни \Rightarrow количество и степени неприводимых делителей $x^n - 1$ можно найти, разбив \mathbb{F}_p на орбиты отображения

$$t \mapsto pt \pmod n.$$

Разложение многочлена $x^{15} - 1$ над полем \mathbb{F}_2 **Пример**

Рассмотрим ещё раз разложение многочлена $x^{15} - 1$ над \mathbb{F}_2 . Относительно умножения на 2 вычеты по модулю 15 разбиваются на такие орбиты:

$$\{\bar{0}\}, \{\bar{1}, \bar{2}, \bar{4}, \bar{8}\}, \{\bar{3}, \bar{6}, \bar{12}, \bar{9}\}, \{\bar{5}, \bar{10}\}, \{\bar{7}, \bar{14}, \bar{13}, \bar{11}\}$$

$$(\bar{12} \cdot 2 = 24 = 15 + \bar{9})$$

Поэтому $x^{15} - 1$ разлагается в произведение

- одного неприводимого многочлена степени 1,
- одного неприводимого многочлена степени 2,
- трех неприводимых многочленов степени 4.

Конкретно (разложение было раньше): $x^{15} + 1 =$
 $= (x + 1)(x^2 + x + 1)(x^4 + x + 1)(x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1).$

Разложение многочлена $x^{23} - 1$ над полем \mathbb{F}_2 **Пример**

Рассмотрим разложение многочлена $x^{23} - 1$ над \mathbb{F}_2 .
Относительно умножения на 2 вычеты по модулю 23
разбиваются на три орбиты:

$$\begin{aligned} & \{ \bar{0} \}, \{ \bar{1}, \bar{2}, \bar{4}, \bar{8}, \bar{16}, \bar{9}, \bar{18}, \bar{13}, \bar{3}, \bar{6}, \bar{12} \}, \\ & \{ \bar{5}, \bar{10}, \bar{20}, \bar{17}, \bar{11}, \bar{22}, \bar{21}, \bar{19}, \bar{15}, \bar{7}, \bar{14} \} \\ & (\bar{18} \cdot 2 = 36 \equiv_{23} \bar{13}) \end{aligned}$$

Поэтому $x^{23} - 1$ разлагается в произведение одного
неприводимого многочлена степени 1 и двух неприводимых
многочленов степени 11.

Разделы

- 1 Поля вычетов по модулю простого числа
- 2 Вычисление элементов в конечных полях
- 3 Линейная алгебра над конечным полем
- 4 Корни многочленов над конечным полем
- 5 Существование и единственность поля Галуа из p^n элементов
- 6 Циклические подпространства
- 7 Задачи с решениями**
- 8 Что надо знать

Задача ПГ-1 (теорема Вильсона)

Доказать, что $(p - 1)! \equiv_p -1$ для простого p .

Задача ПГ-1 (теорема Вильсона)

Доказать, что $(p - 1)! \equiv_p -1$ для простого p .

Решение

$p = 2$: — утверждение тривиально.

Задача ПГ-1 (теорема Вильсона)

Доказать, что $(p - 1)! \equiv_p -1$ для простого p .

Решение

$p = 2$: — утверждение тривиально.

$p > 2$: Степени всех элементов мультипликативной циклической группы $\mathbb{F}_p^* = \{1, \dots, p - 1\}$ делят её порядок $p - 1 \Leftrightarrow \forall x \in \mathbb{F}_p^* : (x^{p-1} = 1) \Rightarrow$ все они являются корнями уравнения $x^{p-1} - 1 = 0$.

Других корней у этого уравнения нет (многочлен степени $p - 1$ имеет не больше $p - 1$ корней).

По теореме Виета их произведение равно свободному члену, т.е. -1 .

Задача ПГ-2

Найти $x \equiv_{17} 1^{2006} + 2^{2006} + \dots + 16^{2006}$.

Задача ПГ-2

Найти $x \equiv_{17} 1^{2006} + 2^{2006} + \dots + 16^{2006}$.

Решение

- Рассмотрим мультипликативную циклическую группу $\{1, 2, \dots, 16\}$ поля \mathbb{F}_{17} ;
- $G = \{1^{2006}, 2^{2006}, \dots, 16^{2006}\}$ — циклическая подгруппа порядка k (здесь только k несовпадающих элементов, $k \mid 16$) этой группы.

- Элементы G — корни уравнения

$$x^k - 1 = 0 \quad (*)$$

- Их сумма по теореме Виета есть коэффициент при x^{k-1} в $(*)$, т.е. 0.

Задача ПГ-3

Построить поле из 4-х элементов.

Задача ПГ-3

Построить поле из 4-х элементов.

Решение

Это поле \mathbb{F}_2^2 , оно может быть построено как фактор-кольцо $\mathbb{F}_2[x]/(a(x))$, где $a(x)$ — неприводимый многочлен из $\mathbb{F}_2[x]$ степени 2.

Но такой многочлен только один: $x^2 + x + 1$.

Следовательно, $\mathbb{F}_2^2 = \{0, 1, x, x + 1\}$

Таблицы сложения и умножения в поле:

+	1	x	$x + 1$
1	0	$x + 1$	x
x	$x + 1$	0	1
$x + 1$	x	1	0

\times	1	x	$x + 1$
1	1	x	$x + 1$
x	x	$x + 1$	1
$x + 1$	$x + 1$	1	x

Задача ПГ-4

Производная многочлена $f \neq 0$ над полем характеристики p тождественно равна 0.

Доказать, что этот многочлен приводимый.

Задача ПГ-4

Производная многочлена $f \neq 0$ над полем характеристики p тождественно равна 0.

Доказать, что этот многочлен приводимый.

Решение

- производная монома $(x^n)' = nx^{n-1}$ тождественно равна 0
iff $n \equiv_p 0 \Leftrightarrow p \mid n$;
- $f' = 0 \Rightarrow$ показатели степеней **всех мономов** многочлена f делятся на p ;
- поэтому $f(x) = g(x^p) = g^p(x)$.

Задача ПГ-5

Доказать, что любая функция $f : \mathbb{F}_p^n \rightarrow \mathbb{F}_p^n$ может быть представлена многочленом.

Задача ПГ-5

Доказать, что любая функция $f : \mathbb{F}_p^n \rightarrow \mathbb{F}_p^n$ может быть представлена многочленом.

Решение

Можно, например, использовать интерполяционный многочлен Лагранжа:

$$f(x) = \sum_{a \in \mathbb{F}_p^n} f(a) \frac{\prod_{b \in \mathbb{F}_p^n \setminus \{a\}} (x - b)}{\prod_{b \in \mathbb{F}_p^n \setminus \{a\}} (a - b)}.$$

Задача ПГ-6

Многочлен $x^5 + x^3 + x^2 + 1$ разложить на неприводимые множители над полем вычетов по модулю 2.

Задача ПГ-6

Многочлен $x^5 + x^3 + x^2 + 1$ разложить на неприводимые множители над полем вычетов по модулю 2.

Решение

- 1 $f(x) = x^5 + x^3 + x^2 + 1$, $f(1) = 0 \Rightarrow 1$ — корень f .
- 2 Делим $f(x)$ на $x - 1$, получаем $x^4 + x^3 + x + 1 = f_1(x)$.
- 3 $f_1(1) = 0 \Rightarrow 1$ — корень f_1 ; $\frac{f_1}{x+1} = x^3 + 1 = f_2(x)$.
- 4 $f_2(1) = 0 \Rightarrow 1$ — корень f_2 ; $\frac{f_2}{x+1} = x^2 + x + 1$.
- 5 Многочлен $x^2 + x + 1$ неприводим.

Ответ: $x^5 + x^3 + x^2 + 1 = (x + 1)^3(x^2 + x + 1)$.

Задача ПГ-7

Многочлен $f(x) = x^3 + 2x^2 + 4x + 1 \in \mathbb{F}_5[x]$ разложить на неприводимые множители.

Задача ПГ-7

Многочлен $f(x) = x^3 + 2x^2 + 4x + 1 \in \mathbb{F}_5[x]$ разложить на неприводимые множители.

Решение

$$\textcircled{1} \quad f(2) = 2^3 + 2 \cdot 2^2 + 4 \cdot 2^2 + 1 = 25 \equiv_5 0, \quad (x - 2) \equiv_5 (x + 3)$$

$\textcircled{2}$

$$\begin{array}{r|l} x^3 + 2x^2 + 4x + 1 & x + 3 \\ \underline{x^3 + 3x^2} & \underline{x^2 + 4x + 2} \\ 4x^2 + 4x & \\ \underline{4x^2 + 2x} & \\ 2x + 1 & \\ \underline{2x + 1} & \\ 0 & \end{array}$$

$$\textcircled{3} \quad \text{многочлен } f_1 = x^2 + 4x + 2 \text{ неприводим в } \mathbb{F}_5$$

Ответ: $x^3 + 2x^2 + 4x + 1 = (x + 3)(x^2 + 4x + 2)$.

Задача ПГ-8

Многочлен $f(x) = x^4 + x^3 + x + 2 \in \mathbb{F}_3[x]$ разложить на неприводимые множители.

Задача ПГ-8

Многочлен $f(x) = x^4 + x^3 + x + 2 \in \mathbb{F}_3[x]$ разложить на неприводимые множители.

Решение

- 0, 1, 2 — не корни $f(x) \Rightarrow f(x)$ линейных делителей не содержит.
- Неприводимые многочлены над \mathbb{F}_3 степени 2:

$$x^2 + 1,$$

$$x^2 + x + 2,$$

$$x^2 + 2x + 2.$$

- Подбором получаем: $f(x) = (x^2 + 1)(x^2 + x + 2)$.

Ответ: $(x^2 + 1)(x^2 + x + 2)$.

Задача ПГ-9

Многочлен $x^4 + 3x^3 + 2x^2 + x + 4$ разложить на неприводимые множители над полем вычетов по модулю 5.

Задача ПГ-9

Многочлен $x^4 + 3x^3 + 2x^2 + x + 4$ разложить на неприводимые множители над полем вычетов по модулю 5.

Решение

1. Убеждаемся, что многочлен $f(x) = x^4 + 3x^3 + 2x^2 + x + 4$ не имеет **линейных** делителей:

$f(x) \neq 0$ ни при одном $x = 0, 1, 2, 3, 4$.

2. Перебирая неприводимые многочлены степени 2 над \mathbb{F}_5 , получаем

$$f(x) = (x^2 + x + 1)(x^2 + 2x + 4).$$

Задача ПГ-10

Разложить на неприводимые множители над полем вычетов по модулю 2 все нормированные многочлены второй степени от x .

Задача ПГ-10

Разложить на неприводимые множители над полем вычетов по модулю 2 все нормированные многочлены второй степени от x .

Решение

$$f_1(x) = x^2 = x \cdot x,$$

$$f_2(x) = x^2 + 1 = (x + 1)^2,$$

$$f_3(x) = x^2 + x = x \cdot (x + 1),$$

$$f_4(x) = x^2 + x + 1 — \text{неприводим.}$$

Задача ПГ-11

Разложить на неприводимые множители все нормированные многочлены третьей степени из $\mathbb{F}_2[x]$.

Задача ПГ-11

Разложить на неприводимые множители все нормированные многочлены третьей степени из $\mathbb{F}_2[x]$.

Решение

$$f_1(x) = x^3,$$

$$f_2(x) = x^3 + 1 = (x + 1)(x^2 + x + 1),$$

$$f_3(x) = x^3 + x = x(x + 1)^2,$$

$$f_4(x) = x^3 + x^2 = x^2(x + 1),$$

$$f_5(x) = x^3 + x + 1 - \text{неприводим},$$

$$f_6(x) = x^3 + x^2 + 1 - \text{неприводим},$$

$$f_7(x) = x^3 + x^2 + x = x(x^2 + x + 1),$$

$$f_8(x) = x^3 + x^2 + x + 1 = (x + 1)^3.$$

Задача ПГ-12

Найти все нормированные многочлены второй степени от x , неприводимые над полем вычетов по модулю 3.

Задача ПГ-12

Найти все нормированные многочлены второй степени от x , неприводимые над полем вычетов по модулю 3.

Решение

Должно быть: $f(0) \neq 0$, $f(1) \neq 0$, $f(2) \neq 0$.

Задача ПГ-12

Найти все нормированные многочлены второй степени от x , неприводимые над полем вычетов по модулю 3.

Решение

Должно быть: $f(0) \neq 0$, $f(1) \neq 0$, $f(2) \neq 0$.

Перебором коэффициентов в выражении $x^2 + bx + c$, находим подходящие многочлены:

$$f_1(x) = x^2 + 1,$$

$$f_2(x) = x^2 + x + 2,$$

$$f_3(x) = x^2 + 2x + 2.$$

Задача ПГ-13

Найти все нормированные многочлены третьей степени от x , неприводимые над полем вычетов по модулю 3.

Задача ПГ-13

Найти все нормированные многочлены третьей степени от x , неприводимые над полем вычетов по модулю 3.

Решение

Должно быть: $f(0) \neq 0$, $f(1) \neq 0$, $f(2) \neq 0$.

Задача ПГ-13

Найти все нормированные многочлены третьей степени от x , неприводимые над полем вычетов по модулю 3.

Решение

Должно быть: $f(0) \neq 0$, $f(1) \neq 0$, $f(2) \neq 0$.

$$f_1(x) = x^3 + 2x + 1,$$

$$f_2(x) = x^3 + 2x + 2,$$

$$f_3(x) = x^3 + x^2 + 2,$$

$$f_4(x) = x^3 + 2x^2 + 1,$$

$$f_5(x) = x^3 + x^2 + x + 2,$$

$$f_6(x) = x^3 + x^2 + 2x + 1,$$

$$f_7(x) = x^3 + 2x^2 + x + 1,$$

$$f_8(x) = x^3 + 2x^2 + 2x + 2.$$

Задача ПГ-14

- 1 Проверить, что $F = \mathbb{F}_7[x]/(x^2 + x - 1)$ является полем.
- 2 Выразить обратный к $1 - x$ в F в базисе $\{\bar{1}, \bar{x}\}$.

Задача ПГ-14

- 1 Проверить, что $F = \mathbb{F}_7[x]/(x^2 + x - 1)$ является полем.
- 2 Выразить обратный к $1 - x$ в F в базисе $\{\bar{1}, \bar{x}\}$.

Решение

1 $a(x) = x^2 + x - 1$, $a(0) = 6$, $a(1) = 1$, $a(2) = 5$, $a(3) = 4$,
 $a(4) = 6$, $a(5) = 1$, $a(6) = 6 \Rightarrow$
многочлен $a(x)$ — неприводим в \mathbb{F}_7 и F — поле ($\cong \mathbb{F}_7^2$).

Задача ПГ-14

- 1 Проверить, что $F = \mathbb{F}_7[x]/(x^2 + x - 1)$ является полем.
- 2 Выразить обратный к $1 - x$ в F в базисе $\{\bar{1}, \bar{x}\}$.

Решение

1 $a(x) = x^2 + x - 1$, $a(0) = 6$, $a(1) = 1$, $a(2) = 5$, $a(3) = 4$,
 $a(4) = 6$, $a(5) = 1$, $a(6) = 6 \Rightarrow$
 многочлен $a(x)$ — неприводим в \mathbb{F}_7 и F — поле ($\cong \mathbb{F}_7^2$).

2
$$\mathbb{F}_7^2 = \{ax + b \mid a, b \in \mathbb{F}_7, x^2 = 1 - x = 6x + 1\}$$

$$(ax + b) \cdot (6x + 1) = \dots = (2a + 6b)x + (6a + b) = 1$$

$$\begin{cases} 6a + b = 1 \\ a + 3b = 0 \end{cases} \Rightarrow \begin{cases} a = 1 \\ b = 2 \end{cases}$$

Проверка: $(6x + 1)(x + 2) = 6x^2 + 13x + 2 = 1 + 7x = 1.$

Задача ПГ-15

Найти порядок элемента $x + x^2$ в мультипликативной группе

- 1 поля $\mathbb{F}_2[x]/(x^4 + x + 1)$;
- 2 поля $\mathbb{F}_2[x]/(x^4 + x^3 + 1)$.

Задача ПГ-15

Найти порядок элемента $x + x^2$ в мультипликативной группе

- 1 поля $\mathbb{F}_2[x]/(x^4 + x + 1)$;
- 2 поля $\mathbb{F}_2[x]/(x^4 + x^3 + 1)$.

Решение $x + x^2 = x(x + 1)$

1 $x^4 = x + 1$

$$(x^2 + x)^2 = x^4 + x^2 = x^2 + x + 1,$$

$$\begin{aligned}(x^2 + x)^3 &= x(x + 1)(x^2 + x + 1) = x(x^3 + 1) = \\ &= x^4 + x = x + 1 + x = 1.\end{aligned}$$

Ответ: 3.

Задача ПГ-15...

Решение

$$\textcircled{2} \quad \underline{x^4 = x^3 + 1}$$

$$(x^2 + x)^2 = x^4 + x^2 = x^3 + x^2 + 1,$$

$$\begin{aligned}(x^2 + x)^3 &= x(x+1)(x^3 + x^2 + 1) = x(x^4 + x^2 + x + 1) = \\ &= x(x^3 + x^2 + x) = x^4 + x^3 + x^2 = x^2 + 1,\end{aligned}$$

$$\begin{aligned}(x^2 + x)^4 &= (x^2 + x)(x^2 + x)^3 = (x^2 + x)(x^2 + 1) = \\ &= x^4 + x^2 + x^3 + x = x^3 + 1 + x^2 + x^3 + x = \\ &= x^2 + x + 1,\end{aligned}$$

...

— ДОЛГО И СЛОЖНО

Задача ПГ-15... $\alpha^4 = \alpha^3 + 1, x = \alpha, \beta = \alpha^2 + \alpha$ Решение

$$\alpha^4 = \alpha^3 + 1$$

$$\alpha^5 = \alpha^4 + \alpha = \alpha^3 + \alpha + 1$$

$$\alpha^6 = \alpha^2(\alpha^3 + 1) = \alpha^3 + \alpha^2 + \alpha + 1$$

$$\alpha^7 = \alpha^4 + \alpha^3 + \alpha^2 + \alpha = \alpha^2 + \alpha + 1$$

$$\alpha^8 = \alpha^3 + \alpha^2 + \alpha$$

$$\alpha^9 = \alpha^4 + \alpha^3 + \alpha^2 = \alpha^2 + 1$$

$$\alpha^{10} = \alpha^3 + 1$$

$$\alpha^{11} = \alpha^4 + \alpha^2 = \alpha^3 + \alpha^2 + 1$$

$$\alpha^{12} = \alpha^4 + \alpha^3 + \alpha = \alpha + 1$$

$$\alpha^{13} = \alpha^2 + \alpha = \beta. \quad 13 \not\mid 15 \Rightarrow \deg \beta = 15$$

Задача ПГ-16

Найти количество неприводимых многочленов

- 1 степени 7 над полем \mathbb{F}_2 ;
- 2 степени 6 над полем \mathbb{F}_5 ;
- 3 степени 24 над полем \mathbb{F}_3 .

Задача ПГ-16

Найти количество неприводимых многочленов

- 1 степени 7 над полем \mathbb{F}_2 ;
- 2 степени 6 над полем \mathbb{F}_5 ;
- 3 степени 24 над полем \mathbb{F}_3 .

Решение

$$\sum_{m|n} md_m = p^n$$

- 1 $d_7 = ?$

$$\sum_{m|7} md_m = 2^7 = 1 \cdot d_1 + 7 \cdot d_7 = 128.$$

$$d_1 = 2 \quad (x, x+1) \Rightarrow d_7 = (128 - 2)/7 = 126/7 = 18.$$

Задача ПГ-17

Чему равно произведение всех *ненулевых* элементов поля \mathbb{F}_2^6 ?

Задача ПГ-17

Чему равно произведение всех *ненулевых* элементов поля \mathbb{F}_2^6 ?

Решение

Все ненулевые элементы поля \mathbb{F}_2^6 являются корнями уравнения

$$x^{2^6-1} - 1 = x^{63} - 1 = 0.$$

По теореме Виета их произведение равно свободному члену, т.е. $-1 \equiv_2 1$.

Задача ПГ-18

Чему равна сумма всех элементов поля \mathbb{F}_3^7 ?

Задача ПГ-18

Чему равна сумма всех элементов поля \mathbb{F}_3^7 ?

Решение

Все элементы поля \mathbb{F}_3^7 являются корнями уравнения

$$x^{3^7} - x = x^{2187} - x = 0. \quad (*)$$

По теореме Виета их сумма равна коэффициенту перед x^{2186} , т.е. 0 .

Задача ПГ-19

Для поля $F = \mathbb{F}_3[x]/(-2x^2 + x + 2)$ построить таблицу соответствий между полиномиальным и степенным представлением для ненулевых элементов.

С помощью данной таблицы вычислить выражение

$$\frac{1}{2x+1} - \frac{(2x)^7(2)}{(x)^9(x+2)}.$$

Задача ПГ-19

Для поля $F = \mathbb{F}_3[x]/(-2x^2 + x + 2)$ построить таблицу соответствий между полиномиальным и степенным представлением для ненулевых элементов.

С помощью данной таблицы вычислить выражение

$$\frac{1}{2x+1} - \frac{(2x)^7(2)}{(x)^9(x+2)}.$$

Решение

$\text{char } F = 3$, поэтому $-2x^2 + x + 2 \equiv_3 x^2 + x + 2 = a(x)$.

F^* содержит $3^2 - 1 = 8$ элементов и все они могут быть представлены как степени $\alpha^i, i = \overline{1, 8}$ примитивного элемента α .

Задача ПГ-19

Для поля $F = \mathbb{F}_3[x]/(-2x^2 + x + 2)$ построить таблицу соответствий между полиномиальным и степенным представлением для ненулевых элементов.

С помощью данной таблицы вычислить выражение

$$\frac{1}{2x+1} - \frac{(2x)^7(2)}{(x)^9(x+2)}.$$

Решение

$\text{char } F = 3$, поэтому $-2x^2 + x + 2 \equiv_3 x^2 + x + 2 = a(x)$.

F^* содержит $3^2 - 1 = 8$ элементов и все они могут быть представлены как степени $\alpha^i, i = \overline{1, 8}$ примитивного элемента α .

Если элемент x окажется примитивным, то положим $\alpha = x$ и, поскольку вычисления в \mathbb{F}_3^2 проводятся по $\text{mod } a(x)$, будем иметь $x^2 + x + 2 = 0 \Rightarrow x^2 = -x - 2 = 2x + 1$.

Задача ПГ-19... $x^2 = 2x + 1, \mathbb{F}_3[x]$ Решение

Найдём порядок элемента $x \Rightarrow$ проверим степени, являющиеся делителями 8, т.е. 2 и 4:

$$x^2 = 2x + 1 \neq 1, \quad x^4 = 2 \neq 1$$

— т.е. x — примитивный элемент F .

Повезло: $a(x) = x^2 + x + 2$ оказался примитивным многочленом над \mathbb{F}_3 (т.е. $a(x) \mid x^8 + 1$ и $a(x) \nmid x^t + 1, t = 3, \dots, 7$), иначе генератор F пришлось бы искать.

Задача ПГ-19... $x^2 = 2x + 1, \mathbb{F}_3[x]$ Решение

Найдём порядок элемента $x \Rightarrow$ проверим степени, являющиеся делителями 8, т.е. 2 и 4:

$$x^2 = 2x + 1 \neq 1, \quad x^4 = 2 \neq 1$$

— т.е. x — примитивный элемент F .

Повезло: $a(x) = x^2 + x + 2$ оказался примитивным многочленом над \mathbb{F}_3 (т.е. $a(x) \mid x^8 + 1$ и $a(x) \nmid x^t + 1, t = 3, \dots, 7$), иначе генератор F пришлось бы искать.

Теперь вычислим значение выражения ($2^8 = 256 \equiv_3 1$):

$$\begin{aligned} \frac{1}{2x+1} - \frac{(2x)^7(2)}{(x)^9(x+2)} &= \frac{1}{x^2} - \frac{x^7}{x^9x^6} = \frac{x^8}{x^2} - \frac{x^7x^8}{x^{15}} = \\ &= x^6 - 1 = x + 2 - 1 = x + 1. \end{aligned}$$

Задача ПГ-20

Для поля $F = \mathbb{F}_3[x]/(x^2 + 1) \cong \mathbb{F}_3^2$ построить таблицу соответствий между полиномиальным и степенным представлением для всех ненулевых элементов поля.

Задача ПГ-20

Для поля $F = \mathbb{F}_3[x]/(x^2 + 1) \cong \mathbb{F}_3^2$ построить таблицу соответствий между полиномиальным и степенным представлением для всех ненулевых элементов поля.

Решение

В данном 9-элементном поле $x^2 + 1 = 0 \Rightarrow x^2 = -1 \equiv_3 2$.

1. Найдём порядок элемента $x \Rightarrow$ проверим степени, являющиеся делителями $9 - 1 = 8$, т.е. 2 и 4:

$$x^2 = 2, \quad x^4 = 1.$$

Следовательно, элемент $\deg x = 4$ и x не является генератором группы F^* ($x^4 - 1 = x^4 + 2 = (x^2 + 1)(x^2 + 2)$ и $x^2 + 1$ — не есть примитивный многочлен над \mathbb{F}_3).

Также не являются примитивными все степени x :

$$x^2 = 2, \quad x^3 = 2x, \quad x^4 = 1.$$

Задача ПГ-20... $x^2 \equiv_3 2$

2. Найдём порядок элемента $x + 1$:

$$(x + 1)^2 = x^2 + 2x + 1 = 2x, \quad (x + 1)^4 = (2x)^2 = 2,$$

т.е. $\alpha = x + 1$ оказался **примитивным элементом**.

Задача ПГ-20... $x^2 \equiv_3 2$

2. Найдём порядок элемента $x + 1$:

$$(x + 1)^2 = x^2 + 2x + 1 = 2x, \quad (x + 1)^4 = (2x)^2 = 2,$$

т.е. $\alpha = x + 1$ оказался **примитивным элементом**.

Его степени:

$$\alpha^1 = x + 1,$$

$$\alpha^5 = 2(x + 1) = 2x + 2,$$

$$\alpha^2 = 2x,$$

$$\alpha^6 = \alpha^2 \cdot \alpha^4 = x,$$

$$\alpha^3 = 2x(x + 1) = 2x + 1,$$

$$\alpha^7 = x(x + 1) = x + 2,$$

$$\alpha^4 = 2,$$

$$\alpha^8 = (\alpha^4)^2 = 1.$$

Заметим, что вычисление очередной степени α^{i+j} часто бывает удобным провести как $\alpha^i \cdot \alpha^j$, а не как $\alpha \cdot \alpha^{i+j-1}$.

Задача ПГ-21

В факторкольце $\mathbb{F}_3[x]/(x^4 + 1)$ найти все элементы главного идеала $(x^2 + x + 2)$.

Задача ПГ-21

В факторкольце $\mathbb{F}_3[x]/(x^4 + 1)$ найти все элементы главного идеала $(x^2 + x + 2)$.

Решение

1. Сначала проверим, является ли многочлен $f(x) = x^2 + x + 2$ делителем $x^4 + 1$?

Задача ПГ-21

В факторкольце $\mathbb{F}_3[x]/(x^4 + 1)$ найти все элементы главного идеала $(x^2 + x + 2)$.

Решение

1. Сначала проверим, является ли многочлен

$f(x) = x^2 + x + 2$ делителем $x^4 + 1$?

$$x^4 + 1 = (x^2 + x + 2) \cdot (x^2 + 2x + 2) - \text{да!}$$

Поэтому искомым идеал составят многочлены кольца (т.е. степени не выше 3), кратные $f(x)$:

$$(x^2 + x + 2) = \{(x^2 + x + 2)(ax + b) \mid a, b \in \mathbb{F}_3\}.$$

Проведём умножение:

$$(x^2 + x + 2) \cdot (ax + b) = ax^3 + (a + b)x^2 + (2a + b)x + 2b.$$

Задача ПГ-21...

2. Теперь, перебирая все возможные значения $a, b \in \mathbb{F}_3$, найдём все элементы идеала $(x^2 + x + 2)$:

a	b	$ax^3 + (a + b)x^2 + (2a + b)x + 2b$
0	0	0
0	1	$x^2 + x + 2$
0	2	$2x^2 + 2x + 1$
1	0	$x^3 + x^2 + 2x$
1	1	$x^3 + 2x^2 + 2$
1	2	$x^3 + x + 1$
2	0	$2x^3 + 2x^2 + x$
2	1	$2x^3 + 2x + 2$
2	2	$2x^3 + x^2 + 1$

Задача ПГ-22

В поле $\mathbb{F}_7[x]/(x^4 + x^3 + x^2 + 3)$ найти обратный к элемент.

Задача ПГ-22

В поле $\mathbb{F}_7[x]/(x^4 + x^3 + x^2 + 3)$ найти обратный к элемент.

Решение

Обратный элемент к $x^2 + x + 3$ находим, решая уравнение

$$\underbrace{(x^4 + x^3 + x^2 + 3) \cdot \chi(x)}_{=0} + (x^2 + x + 3) \cdot y(x) = 1 \quad (*)$$

с помощью расширенного алгоритма Евклида: им будет $y(x)$.

Замечание: вычислять коэффициент при $x^4 + x^3 + x^2 + 3$ ($\chi_i(x)$) нет необходимости.

Задача ПГ-22

Шаг 0. $r_{-2}(x) = x^4 + x^3 + x^2 + 3$, // Инициализация
 $r_{-1}(x) = x^2 + x + 3$,
 $y_{-2}(x) = 0$,
 $y_{-1}(x) = 1$.

Шаг 1. $r_{-2}(x) = r_{-1}(x)q_0(x) + r_0(x)$,
// Делим $r_{-2}(x)$ на $r_{-1}(x)$ с остатком
 $q_0(x) = x^2 + 5$,
 $r_0(x) = 2x + 2$,
 $y_0(x) = y_{-2}(x) - y_{-1}(x)q_0(x) = -q_0(x) = -x^2 - 5$.

Шаг 2. $r_{-1}(x) = r_0(x)q_1(x) + r_1(x)$,
// Делим $r_{-1}(x)$ на $r_0(x)$ с остатком
 $q_1(x) = 4x$,
 $r_1(x) = 3$,
 $y_1(x) = y_{-1}(x) - y_0(x)q_1(x) = 1 + 4x(x^2 + 5) =$
 $= 4x^3 + 6x + 1$.

Задача ПГ-22

Алгоритм заканчивает свою работу на [Шаге 2](#), т.к. степень 0 очередного остатка $r_1(x) = 3$ равна степени многочлена в правой части (*): 1 — [многочлен 0-й степени](#).

Задача ПГ-22

Алгоритм заканчивает свою работу на [Шаге 2](#), т.к. степень 0 очередного остатка $r_1(x) = 3$ равна степени многочлена в правой части (*): 1 — [многочлен 0-й степени](#).

В результате работы алгоритма получено:

$$(x^2 + x + 3)(4x^3 + 6x + 1) = r_1(x) = 3.$$

Задача ПГ-22

Алгоритм заканчивает свою работу на [Шаге 2](#), т.к. степень 0 очередного остатка $r_1(x) = 3$ равна степени многочлена в правой части (*): 1 — **многочлен 0-й степени**.

В результате работы алгоритма получено:

$$(x^2 + x + 3)(4x^3 + 6x + 1) = r_1(x) = 3.$$

Чтобы найти $y(x)$, нужно домножить $y_1(x)$ на $3^{-1} = 5$:

$$y(x) = 5y_1(x) = 5 \cdot (4x^3 + 6x + 1) = 6x^3 + 2x + 5.$$

Задача ПГ-22

Алгоритм заканчивает свою работу на [Шаге 2](#), т.к. степень 0 очередного остатка $r_1(x) = 3$ равна степени многочлена в правой части (*): 1 — **многочлен 0-й степени**.

В результате работы алгоритма получено:

$$(x^2 + x + 3)(4x^3 + 6x + 1) = r_1(x) = 3.$$

Чтобы найти $y(x)$, нужно домножить $y_1(x)$ на $3^{-1} = 5$:

$$y(x) = 5y_1(x) = 5 \cdot (4x^3 + 6x + 1) = 6x^3 + 2x + 5.$$

Проверка: $y(x)(x^2 + x + 3) = (6x^3 + 2x + 5)(x^2 + x + 3) =$
 $= 6x^5 + 6x^4 + 6x^3 + 4x + 1 =$
 $= 6x(-x^3 - x^2 - 3) + 6x^4 + 6x^3 + 4x + 1 = 1.$

Задача ПГ-23

В поле $F = \mathbb{F}_5[x]/(x^2 + 3x + 3)$ найти обратную для матрицы

$$M = \begin{pmatrix} 3x + 4 & x + 2 \\ x + 3 & 3x + 2 \end{pmatrix}.$$

Задача ПГ-23

В поле $F = \mathbb{F}_5[x]/(x^2 + 3x + 3)$ найти обратную для матрицы

$$M = \begin{pmatrix} 3x + 4 & x + 2 \\ x + 3 & 3x + 2 \end{pmatrix}.$$

Решение

Для матриц размера 2×2 обратная матрица записывается в виде

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

1. Сначала вычислим $\det M = ad - bc$ с учётом $x^2 = 2x + 2$:

$$\begin{aligned} \det M &= (3x+4)(3x+2) - (x+2)(x+3) = 4x^2 + 3x + 3 - x^2 - 1 = \\ &= 3x^2 + 3x + 2 = 3(2x + 2) + 3x + 2 = 4x + 3. \end{aligned}$$

Задача ПГ-23...

2. Найдём обратный к $4x + 3$ элемент, решая уравнение

$$(x^2 + 3x + 3) \cdot \chi(x) + (4x + 3) \cdot y(x) = 1.$$

с помощью расширенного алгоритма Евклида:

Шаг 0. $r_{-2}(x) = x^2 + 3x + 3$, // Инициализация

$$r_{-1}(x) = 4x + 3,$$

$$y_{-2}(x) = 0,$$

$$y_{-1}(x) = 1.$$

Шаг 1. $r_{-2}(x) = r_{-1}(x)q_0(x) + r_0(x)$,

// Делим $r_{-2}(x)$ на $r_{-1}(x)$ с остатком

$$q_0(x) = 4x + 4,$$

$$r_0(x) = 1,$$

$$\begin{aligned} y_0(x) &= y_{-2}(x) - y_{-1}(x)q_0(x) = -q_0(x) = \\ &= -4x - 4 = x + 1. \end{aligned}$$

Т.е. $(4x + 3)^{-1} = y_0(x) = x + 1$.

Задача ПГ-23... $x^2 \equiv_5 2x + 2$

3. Вычислим обратную матрицу

$$M^{-1} = (x + 1) \begin{pmatrix} 3x + 2 & 4x + 3 \\ 4x + 2 & 3x + 4 \end{pmatrix} = \begin{pmatrix} x + 3 & 1 \\ 4x & 3x \end{pmatrix}.$$

Задача ПГ-23... $x^2 \equiv_5 2x + 2$

3. Вычислим обратную матрицу

$$M^{-1} = (x + 1) \begin{pmatrix} 3x + 2 & 4x + 3 \\ 4x + 2 & 3x + 4 \end{pmatrix} = \begin{pmatrix} x + 3 & 1 \\ 4x & 3x \end{pmatrix}.$$

Проверка:

$$\begin{aligned} & \begin{pmatrix} 3x + 4 & x + 2 \\ x + 3 & 3x + 2 \end{pmatrix} \times \begin{pmatrix} x + 3 & 1 \\ 4x & 3x \end{pmatrix} = \\ & = \begin{pmatrix} (3x + 4)(x + 3) + 4x(x + 2) & 3x + 4 + 3x(x + 2) \\ (x + 3)^2 + 4x(3x + 2) & x + 3 + 3x(3x + 2) \end{pmatrix} = \\ & = \begin{pmatrix} 2x^2 + x + 2 & 3x^2 + 4x + 4 \\ 3x^2 + 4x + 4 & 4x^2 + 2x + 3 \end{pmatrix} = \\ & = \begin{pmatrix} 2(2x + 2) + x + 2 & 3(2x + 2) + 4x + 4 \\ 3(2x + 2) + 4x + 4 & 4(2x + 2) + 2x + 3 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \end{aligned}$$

Задача ПГ-24

Разложить на неприводимые множители многочлен

$$f(x) = x^{11} + x^9 + x^8 + x^4 + x^3 + x^2 + 1 \in \mathbb{F}_2[x].$$

Задача ПГ-24

Разложить на неприводимые множители многочлен

$$f(x) = x^{11} + x^9 + x^8 + x^4 + x^3 + x^2 + 1 \in \mathbb{F}_2[x].$$

Решение

1. Сначала пытаемся найти корни $f(x)$ в \mathbb{F}_2 :

$$f(0) = 1, \quad f(1) = 1.$$

Значит, $f(x)$ не имеет корней в \mathbb{F}_2 т.е. не имеет **линейных** множителей.

Задача ПГ-24

Разложить на неприводимые множители многочлен

$$f(x) = x^{11} + x^9 + x^8 + x^4 + x^3 + x^2 + 1 \in \mathbb{F}_2[x].$$

Решение

1. Сначала пытаемся найти корни $f(x)$ в \mathbb{F}_2 :

$$f(0) = 1, \quad f(1) = 1.$$

Значит, $f(x)$ не имеет корней в \mathbb{F}_2 т.е. не имеет **линейных** множителей.

2. Далее ищем делители $f(x)$ среди неприводимых многочленов степени 2.

Таковых над \mathbb{F}_2 только один — $x^2 + x + 1$.

При делении $f(x)$ на $x^2 + x + 1$, получаем

$$f(x) = (x^2 + x + 1)(x^9 + x^8 + x^7 + x^6 + x^4 + x^3 + x^2 + x + 1).$$

Задача ПГ-24...

Продолжаем дальше делить на $x^2 + x + 1$:

$$\begin{aligned}g(x) &= x^9 + x^8 + x^7 + x^6 + x^4 + x^3 + x^2 + x + 1 = \\ &= (x^2 + x + 1)(x^7 + x^4 + x^3 + x^2 + x + 1) + x,\end{aligned}$$

т.е. $x^2 + x + 1$ — делитель $f(x)$ кратности 1.

Задача ПГ-24...

Продолжаем дальше делить на $x^2 + x + 1$:

$$\begin{aligned} g(x) &= x^9 + x^8 + x^7 + x^6 + x^4 + x^3 + x^2 + x + 1 = \\ &= (x^2 + x + 1)(x^7 + x^4 + x^3 + x^2 + x + 1) + x, \end{aligned}$$

т.е. $x^2 + x + 1$ — делитель $f(x)$ кратности 1.

3. Неприводимых многочленов степени 3 над \mathbb{F}_2 два:

$x^3 + x + 1$ и $x^3 + x^2 + 1$.

Попробуем поделить $g(x)$ на $x^3 + x + 1$:

$$\begin{aligned} x^9 + x^8 + x^7 + x^6 + x^4 + x^3 + x^2 + x + 1 &= \\ &= (x^3 + x + 1)(x^6 + x^5 + x^3 + x^2 + 1) \end{aligned}$$

— делится!

Задача ПГ-24...

Производя далее попытки деления $h(x) = x^6 + x^5 + x^3 + x^2 + 1$ на многочлены 3-й степени, получаем

$$x^6 + x^5 + x^3 + x^2 + 1 = (x^3 + x + 1)(x^3 + x^2 + x + 1) + x^2,$$

$$x^6 + x^5 + x^3 + x^2 + 1 = (x^3 + x^2 + 1)x^3 + x^2 + 1.$$

Задача ПГ-24...

Производя далее попытки деления $h(x) = x^6 + x^5 + x^3 + x^2 + 1$ на многочлены 3-й степени, получаем

$$x^6 + x^5 + x^3 + x^2 + 1 = (x^3 + x + 1)(x^3 + x^2 + x + 1) + x^2,$$

$$x^6 + x^5 + x^3 + x^2 + 1 = (x^3 + x^2 + 1)x^3 + x^2 + 1.$$

Т.к. как многочлен 6-ой степени $h(x)$ не имеет делителей 3-й и меньших степеней, то он является неприводимым: если бы он имел делитель, скажем, степени 4, то у него был бы и делитель степени $6 - 4 = 2$.

Задача ПГ-24...

Производя далее попытки деления $h(x) = x^6 + x^5 + x^3 + x^2 + 1$ на многочлены 3-й степени, получаем

$$x^6 + x^5 + x^3 + x^2 + 1 = (x^3 + x + 1)(x^3 + x^2 + x + 1) + x^2,$$

$$x^6 + x^5 + x^3 + x^2 + 1 = (x^3 + x^2 + 1)x^3 + x^2 + 1.$$

Т.к. как многочлен 6-ой степени $h(x)$ не имеет делителей 3-й и меньших степеней, то он является неприводимым: если бы он имел делитель, скажем, степени 4, то у него был бы и делитель степени $6 - 4 = 2$.

В итоге в $\mathbb{F}_2[x]$ имеем разложение

$$\begin{aligned} f(x) &= x^{11} + x^9 + x^8 + x^4 + x^3 + x^2 + 1 = \\ &= (x^2 + x + 1)(x^3 + x + 1)(x^6 + x^5 + x^3 + x^2 + 1). \end{aligned}$$

Задача ПГ-25

Найти минимальное поле характеристики 3, в котором многочлен $f(x) = x^3 + x + 2 \in \mathbb{F}_3[x]$ раскладывается на линейные множители.

В данном поле найти все корни данного многочлена.

Задача ПГ-25

Найти минимальное поле характеристики 3, в котором многочлен $f(x) = x^3 + x + 2 \in \mathbb{F}_3[x]$ раскладывается на линейные множители.

В данном поле найти все корни данного многочлена.

Решение

1. Найдём разложение многочлена $f(x)$ на неприводимые множители над \mathbb{F}_3 .

- Проверяем корни: $f(0) = 2$, $f(1) = 1$, $f(2) = 0$.
Т.к. $x - 2 \equiv_3 x + 1$, то $f(x) = (x + 1)(x^2 + 2x + 2)$.
- Найдём разложение многочлена $g(x) = x^2 + 2x + 2 \in \mathbb{F}_3[x]$.
Он не имеет корней, его степень = 2 \Rightarrow он неприводим.
- Окончательно: $f(x) = (x + 1)(x^2 + 2x + 2)$.

Задача ПГ-25...

2. Известно, что если $g(x)$ — неприводимый многочлен степени n над конечным полем \mathbb{F}_p , то он:

Задача ПГ-25...

2. Известно, что если $g(x)$ — неприводимый многочлен степени n над конечным полем \mathbb{F}_p , то он:

- в поле своего расширения $F = \mathbb{F}_p[x]/(g(x))$ раскладывается на n линейных множителей —

$$g(x) = (x - \alpha) \cdot (x - \alpha^p) \cdot (x - \alpha^{p^2}) \cdot \dots \cdot (x - \alpha^{p^{n-1}}),$$

где α — произвольный корень $g(x)$ в F ;

- не имеет корней ни в каком конечном поле, содержащим менее, чем p^n элементов.

Задача ПГ-25...

2. Известно, что если $g(x)$ — неприводимый многочлен степени n над конечным полем \mathbb{F}_p , то он:

- в поле своего расширения $F = \mathbb{F}_p[x]/(g(x))$ раскладывается на n линейных множителей —

$$g(x) = (x - \alpha) \cdot (x - \alpha^p) \cdot (x - \alpha^{p^2}) \cdot \dots \cdot (x - \alpha^{p^{n-1}}),$$

где α — произвольный корень $g(x)$ в F ;

- не имеет корней ни в каком конечном поле, содержащим менее, чем p^n элементов.

3. Рассмотрим поле $\mathbb{F}_3[x]/(g(x))$ расширения многочлена

$$g(x) = x^2 + 2x + 2.$$

В этом поле если α — корень $g(x)$, то и α^3 — тоже корень.

Вычисляем:

$$\alpha^2 = -2\alpha - 2 = \alpha + 1 \text{ и } \alpha^3 = \alpha(\alpha + 1) = \alpha^2 + \alpha = 2\alpha + 1.$$

Задача ПГ-25... $\alpha^2 = \alpha + 1 \in \mathbb{F}_3$

Действительно (подчёркиваем слагаемые, дающие в сумме 0):

$$\begin{aligned}(x - \alpha)(x - 2\alpha - 1) &= (x + 2\alpha) \cdot (x + \alpha + 2) = \\ &= x^2 + \underline{\alpha x} + 2x + \underline{2\alpha x} + 2\alpha^2 + 4\alpha = \\ &= x^2 + 2x + \underline{2\alpha} + 2 + \underline{4\alpha} = x^2 + 2x + 2.\end{aligned}$$

Задача ПГ-25... $\alpha^2 = \alpha + 1 \in \mathbb{F}_3$

Действительно (подчёркиваем слагаемые, дающие в сумме 0):

$$\begin{aligned}(x - \alpha)(x - 2\alpha - 1) &= (x + 2\alpha) \cdot (x + \alpha + 2) = \\ &= x^2 + \underline{\alpha x} + 2x + \underline{2\alpha x} + 2\alpha^2 + 4\alpha = \\ &= x^2 + 2x + \underline{2\alpha} + 2 + \underline{4\alpha} = x^2 + 2x + 2.\end{aligned}$$

Построенное расширение — поле $\mathbb{F}_3[x]/(x^2 + 2x + 2)$ — содержит найденный ранее корень 2, поэтому многочлен $f(x)$ в этом поле раскладывается на следующие линейные множители:

$$\begin{aligned}f(x) &= x^3 + x + 2 = (x - 2)(x - \alpha)(x - 2\alpha - 1) = \\ &= (x + 1)(x + 2\alpha)(x + \alpha + 2).\end{aligned}$$

Задача ПГ-25... \mathbb{F}_3

4. Определить корни многочлена $g(x) = (x - \alpha)(x - 2\alpha - 1)$ в поле $\mathbb{F}_3[x]/(x^2 + 2x + 2)$ легко:

Задача ПГ-25... \mathbb{F}_3

4. Определить корни многочлена $g(x) = (x - \alpha)(x - 2\alpha - 1)$ в поле $\mathbb{F}_3[x]/(x^2 + 2x + 2)$ легко:

всегда можно взять $\alpha = x$,

откуда второй корень $\alpha^3 = 2\alpha + 1 = 2x + 1$.

Задача ПГ-25... \mathbb{F}_3

4. Определить корни многочлена $g(x) = (x - \alpha)(x - 2\alpha - 1)$ в поле $\mathbb{F}_3[x]/(x^2 + 2x + 2)$ легко:

всегда можно взять $\alpha = x$,

откуда второй корень $\alpha^3 = 2\alpha + 1 = 2x + 1$.

5. Таким образом, в поле $\mathbb{F}_3[x]/(x^2 + 2x + 2)$ многочлен $f(x) = x^3 + x + 2$ имеет корни

2, x и $2x + 1$.

Задача ПГ-26...

Найти минимальный многочлен $m(x) \in \mathbb{F}_5[x]$, который имеет корень α^3 , где α — примитивный элемент поля

$$F = \mathbb{F}_5[x]/(x^2 + x + 2).$$

Задача ПГ-26...

Найти минимальный многочлен $m(x) \in \mathbb{F}_5[x]$, который имеет корень α^3 , где α — примитивный элемент поля

$$F = \mathbb{F}_5[x]/(x^2 + x + 2).$$

Решение

1. Известно, что минимальный многочлен $m(x)$ в поле характеристики 5 вместе с корнем α^3 содержит все смежные с ним $(\alpha^3)^5 = \alpha^{15}$, $(\alpha^3)^{5^2} = \alpha^{75}$, $(\alpha^3)^{5^3} = \alpha^{375}$ и т.д.

Задача ПГ-26...

Найти минимальный многочлен $m(x) \in \mathbb{F}_5[x]$, который имеет корень α^3 , где α — примитивный элемент поля

$$F = \mathbb{F}_5[x]/(x^2 + x + 2).$$

Решение

1. Известно, что минимальный многочлен $m(x)$ в поле характеристики 5 вместе с корнем α^3 содержит все смежные с ним $(\alpha^3)^5 = \alpha^{15}$, $(\alpha^3)^{5^2} = \alpha^{75}$, $(\alpha^3)^{5^3} = \alpha^{375}$ и т.д.

2. В поле F_5^2 будет $\alpha^{5^2-1} = \alpha^{24} = 1 \Rightarrow$ смежный класс, образованный α^3 содержит только два элемента α^3 и α^{15} (т.к. $\alpha^{75} = \alpha^{24 \cdot 3 + 3} = \alpha^3$) \Rightarrow минимальный многочлен $m(x)$ имеет степень 2 и может быть представлен как

$$m(x) = (x - \alpha^3)(x - \alpha^{15}) = x^2 - (\alpha^3 + \alpha^{15})x + \alpha^{18}.$$

Задача ПГ-26... $m(x) = x^2 - (\alpha^3 + \alpha^{15})x + \alpha^{18}$

3. Найдём коэффициенты многочлена $m(x)$ учётом $\alpha^2 = -\alpha - 2 = 4\alpha + 3$:

$$\begin{aligned}\alpha^3 &= \alpha \cdot \alpha^2 = \alpha(4\alpha + 3) = 4\alpha^2 + 3\alpha = \\ &= 4(4\alpha + 3) + 3\alpha = 4\alpha + 2,\end{aligned}$$

$$\begin{aligned}\alpha^{15} &= (\alpha^3)^5 = (4\alpha + 2)^5 = 4\alpha^5 + 2 = \\ &= 4\alpha^2\alpha^3 + 2 = 4(4\alpha + 3)(4\alpha + 2) + 2 = \\ &= 4(\alpha^2 + 1) + 2 = 4(4\alpha + 4) + 2 = \alpha + 3,\end{aligned}$$

$$\alpha^3 + \alpha^{15} = 4\alpha + 2 + \alpha + 3 = 0,$$

$$\begin{aligned}\alpha^{18} &= \alpha^3\alpha^{15} = (4\alpha + 2)(\alpha + 3) = \\ &= 4(4\alpha + 3) + 4\alpha + 1 = 3.\end{aligned}$$

Задача ПГ-26... $m(x) = x^2 - (\alpha^3 + \alpha^{15})x + \alpha^{18}$

3. Найдём коэффициенты многочлена $m(x)$ учётом $\alpha^2 = -\alpha - 2 = 4\alpha + 3$:

$$\begin{aligned}\alpha^3 &= \alpha \cdot \alpha^2 = \alpha(4\alpha + 3) = 4\alpha^2 + 3\alpha = \\ &= 4(4\alpha + 3) + 3\alpha = 4\alpha + 2,\end{aligned}$$

$$\begin{aligned}\alpha^{15} &= (\alpha^3)^5 = (4\alpha + 2)^5 = 4\alpha^5 + 2 = \\ &= 4\alpha^2\alpha^3 + 2 = 4(4\alpha + 3)(4\alpha + 2) + 2 = \\ &= 4(\alpha^2 + 1) + 2 = 4(4\alpha + 4) + 2 = \alpha + 3,\end{aligned}$$

$$\alpha^3 + \alpha^{15} = 4\alpha + 2 + \alpha + 3 = 0,$$

$$\begin{aligned}\alpha^{18} &= \alpha^3\alpha^{15} = (4\alpha + 2)(\alpha + 3) = \\ &= 4(4\alpha + 3) + 4\alpha + 1 = 3.\end{aligned}$$

В итоге:

$$m(x) = x^2 + 3.$$

Разделы

- 1 Поля вычетов по модулю простого числа
- 2 Вычисление элементов в конечных полях
- 3 Линейная алгебра над конечным полем
- 4 Корни многочленов над конечным полем
- 5 Существование и единственность поля Галуа из p^n элементов
- 6 Циклические подпространства
- 7 Задачи с решениями
- 8 Что надо знать**

- Конечное поле и его характеристика. Мультипликативная группа, примитивный элемент поля Галуа и его нахождение. Основная теорема алгебры.
- Алгоритм Евклида и его применение. Теорема Безу и расширенный алгоритм Евклида.
- Неприводимые многочлены: существование и нахождение неприводимых многочленов в конечных полях. Построение конечных полей с помощью неприводимых многочленов (привести пример). Изоморфизм конечных полей.
- Векторное пространство многочленов. Базис в \mathbb{F}_p^n . Поля Галуа как векторные пространства. Подполя конечного поля.

- Минимальные многочлены над конечным полем: примеры и свойства. Корнями какого многочлена являются все элементы конечного поля? Делителями какого многочлена являются все неприводимые многочлены n -й степени?
- Теорема о степени любого неприводимого делителя многочлена $x^{p^n-1} - 1$.
- Теорема о корнях неприводимого многочлена. Многочлены над конечным полем: решение уравнений.
- Как решать уравнения, когда корней нет (алгоритм нахождения всех корней многочлена $f(x)$ над полем Галуа \mathbb{F}_p)?
- Мультипликативная группа расширения поля. Существование неприводимого многочлена степени n над полем \mathbb{F}_p .

- Лемма о числе неприводимых нормированных многочленов из \mathbb{F}_p^n . Среднее число неприводимых многочленов.
- Изоморфизм полей Галуа с одинаковым числом элементов.
- Теорема о неприводимом нормированном многочлене — делителе порождающего элемента идеала.
- Циклическое пространство: определение и примеры. Количество и степени неприводимых делителей $x^n - 1$.