Доп. дисциплины. Магистры весна 2021.

Занятие 1

Алгоритмы теории многочленов

11.03.2021

Евклидовы кольца

Определение. *Полем Галуа называется любое конечное поле.*

Поле Галуа и поле ненулевой характеристики – это не синонимы. Любое поле Галуа имеет конечную характеристику. Но любое бесконечное поле ненулевой характеристики не является полем Галуа.

Найдите в кольце Z_8 все решения уравнения 4*x = 4

Конечные кольца, т.е. конечные алгебраические множества, где можно складывать, вычитать и умножать элементы, но не на все ненулевые элементы можно делить, очень своеобразные объекты в сравнении с привычными натуральными и действительными числами.

Поскольку кольцо Z_8 конечное и содержит всего 8 элементов, то можно решить уравнение, просто перебрав все элементы этого кольца. Перебрав все элементы, мы убедимся, что решениями являются все нечетные элементы {1, 3, 5, 7}. Т.е. уравнение первой степени имеет 4 решения.

Другой способ состоит в том, что, если a – решение, то и любой элемент a+2*k, тоже решение. Поскольку a = 1 – решение, то мы сразу получаем и другие решения 1 + 2, 1 + 4, 1 + 6. Остается только проверить, что других решений нет.

В нашем случае оба решения приемлемы. Но если бы кольцо содержало много элементов, то первый способ мог бы оказаться неприменимым.

Сколько различных матриц размера 3Х3 существует над кольцом Z_6 ?

Эта задача похожа на задачу про число функций над некоторым конечным множеством. Матрица размера 3Х3 имеет 9 элементов. Каждый из элементов может принимать любое значение из кольца $\mathbf{Z_6}$**.** В кольце $\mathbf{Z_6}$ всего 6 элементов. Т.к. каждый из 9 элементов матрицы пробегает все эти значения независимо друг от друга, то всего получается 6^9 = 10077696 различных матриц – примерно 10 млн. штук.

Над полем GF(7) найти матрицу, обратную к матрице

$$\begin{pmatrix} 1 & 2 & 3 \\ 0 & 2 & 3 \\ 0 & 0 & 3 \end{pmatrix}.$$

Задача на применение метода Гаусса. Алгоритм нахождения обратной матрицы состоит в том, что нашей матрице мы справа приписываем единичную матрицу такого же размера и элементарными преобразованиями строк приводим исходную матрицу к единичной. Как только это будет сделано, приписанная нами единичная матрица превратится в матрицу, обратную к нашей исходной матрице.

I элементарное преобразование строк над полем. Умножение строки на ненулевой элемент.

II элементарное преобразование строк над полем. Умножение строки на любой элемент и прибавление к другой строке. Иногда добавляют третье преобразование – поменять местами две строки. На самом деле – это не элементарное преобразование, оно может быть заменено некоторой последовательностью первых двух преобразований.

Отметим, что в поле GF(5), над которым мы будем производить преобразования, выполняются равенства $2\cdot 3=1, -1=4, 3\cdot 4=2$.

$$\left\langle \begin{pmatrix} 1 & 2 & 3 \\ 0 & 2 & 3 \\ 0 & 0 & 3 \end{pmatrix} \middle| \begin{matrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{matrix} \right\rangle \Rightarrow \left\langle \begin{pmatrix} 1 & 2 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix} \middle| \begin{matrix} 1 & 0 & 4 \\ 0 & 1 & 4 \\ 0 & 0 & 1 \end{matrix} \right\rangle \Rightarrow \left\langle \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix} \middle| \begin{matrix} 1 & 4 & 0 \\ 0 & 1 & 4 \\ 0 & 0 & 1 \end{matrix} \right\rangle \Rightarrow \left\langle \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \middle| \begin{matrix} 1 & 4 & 0 \\ 0 & 3 & 2 \\ 0 & 0 & 2 \end{matrix} \right\rangle$$

Таким образом, матрицей обратной к исходной будет $\begin{pmatrix} 1 & 4 & 0 \\ 0 & 3 & 2 \\ 0 & 0 & 2 \end{pmatrix}$, что легко проверить непосредственным умножением.

Решить систему линейных уравнений над полем GF(5)

$$\begin{cases} x + y + z = 1 \\ x - z = 0 \\ x - y = 1 \end{cases}.$$

Упражнение на алгоритм Гаусса. Необходимо расширенную матрицу системы линейных уравнений привести элементарным преобразованиями строк к диагональному виду.

На первом шаге в первом столбце нужно выбрать неединичный элемент и строку, в которой он расположен, сделать первой строкой матрицы, переставив ее с другими строками матрицы. После этого используя этот неединичный элемент обнулить весь первый столбец матрицы.

На втором шаге, мысленно вычеркнув 1-ю строку и 1-й столбец, применить первый шаг к матрице, получившейся после этого вычеркивания. Не позднее, чем на n-1 шаге, если матрица имеет размер nXn, у нас получится нужная матрица.

Применим этот алгоритм к расширенной матрице нашей системы линейных уравнений. На первом шаге в качестве основной возьмем 2-ю строку, в ней больше всего нулей, и переместив ее на первое место обнулим первый столбец. Так же заметим, что в поле GF(5) имеет место равенства $2\cdot 3=1, -1=4, 3\cdot 4=2$

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & -1 & 0 \\ 1 & -1 & 0 & 1 \end{pmatrix} \Rightarrow \begin{pmatrix} 1 & 0 & 4 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 4 & 0 & 1 \end{pmatrix} \Rightarrow \begin{pmatrix} 1 & 0 & 4 & 0 \\ 0 & 1 & 2 & 1 \\ 0 & 4 & 1 & 1 \end{pmatrix} \Rightarrow$$

$$\begin{pmatrix} 1 & 0 & 4 & 0 \\ 0 & 1 & 2 & 1 \\ 0 & 0 & 3 & 2 \end{pmatrix} \Rightarrow \begin{pmatrix} 1 & 0 & 4 & 0 \\ 0 & 1 & 2 & 1 \\ 0 & 0 & 1 & 4 \end{pmatrix} \Rightarrow \begin{pmatrix} 1 & 0 & 0 & 4 \\ 0 & 1 & 0 & 3 \\ 0 & 0 & 1 & 4 \end{pmatrix}$$

Итак, получилось решение $\begin{cases} x = 4 \\ y = 3 \\ z = 4 \end{cases}.$

Следствие из алгоритма Евклида. *Если в евклидовом кольце* **d=gcd(a,b),** *то найдутся такие элементы* **u, v,** *что* **d = ua + vb,** *т.е. НОД является линейной комбинацией исходных элементов* **a** и **b**.

По методу Евклида найти элемент обратный к 127 по модулю 256

Задача на использование алгоритма Евклида для нахождения наибольшего общего делителя двух целых чисел. Пусть a и b - натуральные числа. Разделим число «a» с остатком на число «b». Потом число «b» делим на получившийся остаток r и т.д.

Последний остаток r_n и есть наибольший общий делитель чисел a и b. В случае, когда числа a и b взаимно простые последний остаток будет равен 1.

Используя полученные равенства можно выразить элемент r_n через исходные элементы a и b.

Сделаем это для случая, когда n = 3.

$$\begin{cases} a = bq + r \\ b = rq_1 + r_1 \\ r = r_1q_2 + r_2 \\ r_1 = r_2q_3 + r_3 \\ r_2 = r_3q_4 \end{cases} \Rightarrow \begin{cases} r = a - bq \\ r_1 = b - rq_1 \\ r_2 = r - r_1q_2 \\ r_3 = r_1 - r_2q_3 \\ r_2 = r_3q_4 \end{cases} \Rightarrow \begin{cases} r = a - bq = a + (-q)b \\ r_1 = b - (a - bq)q_1 = (-q_1)a + (1 + qq_1)b \\ r_2 = (a - bq) - r_1q_2 \\ r_3 = r_1 - r_2q_3 \\ r_2 = r_3q_4 \end{cases} \Rightarrow$$

$$\begin{cases} r = a + (-q)b \\ r_1 = (-q_1)a + (1 + qq_1)b \\ r_2 = (a - bq) - ((-q_1)a + (1 + qq_1)b)q_2 = (1 + q_1q_2)a + (-q - (1 + qq_1)q_2)b \\ r_3 = ((-q_1)a + (1 + qq_1)b) - ((1 + q_1q_2)a + (-q - (1 + qq_1)q_2)b)q_3 \\ r_2 = r_3q_4 \end{cases} \Rightarrow$$

$$\begin{cases} r = a + (-q)b \\ r_1 = (-q_1)a + (1 + qq_1)b \\ r_2 = (1 + q_1q_2)a + (-q - (1 + qq_1)q_2)b \\ r_3 = ((-q_1)a + (1 + qq_1)b) - ((1 + q_1q_2)a + (-q - (1 + qq_1)q_2)b)q_3 \\ r_2 = r_3q_4 \end{cases} \Rightarrow$$

$$r_3 = (-q_1 - q_3 - q_1q_2q_3)a + (1 + qq_1 + qq_3 + q_2q_3 + qq_1q_2q_3)b$$

Применим этот алгоритм к нашим числам 127 и 256:

$$\begin{cases} \overline{256} = \overline{127} \cdot 2 + \overline{2} \\ \overline{127} = \overline{2} \cdot 63 + \overline{1} \end{cases} \Rightarrow \begin{cases} \overline{256} - \overline{127} \cdot 2 = \overline{2} \\ \overline{127} - \overline{2} \cdot 63 = \overline{1} \end{cases} \Rightarrow \begin{cases} \overline{256} - \overline{127} \cdot 2 = \overline{2} \\ \overline{127} - (\overline{256} - \overline{127} \cdot 2) \cdot 63 = \overline{1} \end{cases} \Rightarrow$$

$$(1 + 2 \cdot 63) \cdot \overline{127} + (-63) \cdot \overline{256} = \overline{1}$$

Таким образом, получаем $127 \cdot 127 - 63 \cdot 256 = 1 \Rightarrow 127 \cdot 127 = 1 + 63 \cdot 256$, т.е. $127 \cdot 127 = 1 (\mathrm{mod}\, 256)$

Значит, элементом обратным по умножению к 127 в кольце вычетов Z_{256} будет сам же элемент 127.

Литература

1. Шевелев Ю.П. Дискретная математика, 4-е изд. [Электронный ресурс]. – СПб.: Лань, 2019. – URL: https://e.lanbook.com/reader/book/118616
2. Глухов М.М., Елизаров В.П., Нечаев А.А. Алгебра, 3-е изд. [Электронный ресурс]. - СПб.: Лань, 2020. - URL: https://e.lanbook.com/reader/book/126718/