КОРНИ МНОГОЧЛЕНОВ НАД КОНЕЧНЫМИ ПОЛЯМИ

Н. М. Жадько,
студент факультета экономики и права
Гомельский филиал Учреждения образования Федерации профсоюзов Беларуси «Международный университет «МИТСО», г. Гомель
Научный руководитель:
В. Н. Тютянов,
доктор физико-атематических наук, профессор
профессор кафедры общенаучных и гуманитарных дисциплин
Гомельский филиал Учреждения образования Федерации профсоюзов Беларуси «Международный университет «МИТСО», г. Гомель

В течение последних десятилетий на развитие ряда прикладных проблем все большее влияние оказывает такой раздел алгебры, как теория конечных полей, а также алгебраические объекты над конечными полями (многочлены, матрицы и другие).

Одной из важнейших областей, в которых применяется теория конечных полей, является теория кодирования. В частности, одним из центральных направлений в данной области является описание избыточных кодов с помощью многочленов над конечным полем. Другим важным разделом теории кодирования является алгебраическая теория кодирования, которая включает изучение различных видов кодов. Сюда относятся линейные и циклические коды, изучение которых опирается на рассмотрение вопросов линейной алгебры над конечными полями.

Отметим также важное приложение конечных полей в криптографии, которая в свою очередь применяется в ряде прикладных дисциплин, в частности в банковском деле. Большое применение в последнее время конечные поля находят в задачах анализа экспериментальных данных, непосредственно применяемого в многочисленных прикладных науках.

Во многих числовых системах, которые применяются в элементарной арифметике, используются две бинарные операции: *сложение* и *умножение*. Примерами таких систем являются целые, рациональные и действительные числа. Мы введем важнейший тип алгебраической структуры, называемый кольцом, в котором сохраняются все основные свойства приведенных выше числовых систем.

Определение 1. *Кольцом* $(R, +, \cdot)$ *называется множество* R *с двумя бинарными операциями, обозначаемыми символами «+» и «·», такими, что*

1. R *– абелева группа относительно операции «+».*

2. Операция ассоциативна, т. е. для всех $a, b, c \in R$

$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$

3. Выполняются законы дистрибутивности, т. е. для всех $a, b, c \in R$

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

и

$$(b + c) \cdot a = b \cdot a + c \cdot a$$

Особо отметим тот факт, что операции *«+» и «·»*не обязательно являются обычными сложением и умножением. Для краткости кольцо $(R, +, \cdot)$ будем обозначать одной буквой R. *Единичный элемент* аддитивной группы кольца R называется *нулевым элементом* (или нулем) кольца R и обозначается символом «0», а обратный к элементу a этой группы обозначается через $-a$. Вместо $a + (-b)$ обычно пишут $a - b$, а вместо $a \cdot b$ – просто ab.

Из определения кольца получается следующее общее свойство $a0 = 0a = 0$ для всех $a \in R$. Из этого можно очень легко получить, что $(-a)\,b = a\,(-b) = -ab$ для всех $a, b \in R$.

Простейшим примером кольца может служить кольцо всех целых чисел. Рассматривая его свойства, нетрудно обнаружить среди них такие, которыми не обладает произвольное кольцо. Это приводит к тому, что кольца допускают дальнейшую классификацию.

Определение 2.

(i) Кольцо называется кольцом с единицей, если оно имеет мультипликативную единицу, т. е. если существует такой элемент $e \in R$, что $ae = ea = a$ для любого $a \in R$.

(ii) Кольцо называется коммутативным, если операция «·»коммутативна.

(iii) Кольцо называется целостным кольцом (или областью целостности), если оно является коммутативным кольцом с единицей $e \neq 0$, в котором равенство $ab = 0$ влечет за собой $a = 0$ или $b = 0$.

(iv) Кольцо R называется телом, если $R \neq \{0\}$ и ненулевые элементы в R образуют группу относительно операции «·».

(v) Коммутативное тело называется полем.

Таким образом, поле есть множество F, на котором заданы две операции, называемые *сложением* и *умножением*, и которое содержит два выделенных элемента 0 и e, причем $e \neq 0$. Далее, поле F – абелева группа по сложению, единичным элементом которой является 0, а элементы из F, отличные от 0, образуют абелеву группу по умножению, единичным элементом которой является e. Две операции, сложение и умножение, связаны законом дистрибутивности $a\cdot(b + c) = a \cdot b + a \cdot c$. Второй закон дистрибутивности $(b + c) \cdot a = b \cdot a + c \cdot a$ выполняется автоматически в силу коммутативности умножения. Элемент 0 называется *нулевым элементом* (или просто нулем), а e – *единичным элементом* (или просто единицей) поля F. В дальнейшем для единицы, как правило, будет использоваться символ 1.

Свойство, появляющееся в определении 2 (*iii*): равенство $ab = 0$ влечет за собой $a = 0$ или $b = 0$ – выражают словами «отсутствуют делители нуля». В частности, поле не имеет делителей нуля, так как если $ab = 0$ и $a \neq 0$, то умножение на a^{-1} дает $b = a^{-1}0 = 0$.

Пусть **P** – некоторое поле. Рассмотрим многочлен степени n над полем: **P** $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, где a_i являются элементами поля **P**. Элемент a из поля **P** называется корнем многочлена $f(x)$, если $f(a) = 0$. В случае, когда **P** является полем рациональных или действительных чисел, то имеются хорошо разработанные методы отыскания корней многочлена с любой заданной точностью.

Мы будем рассматривать случай, когда **P** – конечное поле. Хорошо известно [1, с. 66], что число элементов данного поля является степенью простого числа p, называемого характеристикой поля. Такое поле обозначается $GF(p^n)$ и называется полем Галуа. Важным частным случаем является простое поле, когда $n = 1$. Данное поле обозначается F_p.

Мы рассмотрим задачу быстрого нахождения корней многочлена $f(x)$ над полем F_p. Отметим, что всякое поле содержит нулевой и единичный элементы. В случае поля F_2 все его элементы исчерпываются нулем и единицей. Поле F_p состоит из элементов, $b_0 = 0, b_1 = 1, b_2, \cdots, b_{p-1}$. Данные элементы будем обозначать жирными числами $\mathbf{0}, \mathbf{1}, \mathbf{2}, \cdots, \boldsymbol{p-1}$. Следует заметить, что это не числа в обычном понимании, а некоторые символы. Каждому элементу поля F_p сопоставим естественным способом соответствующее ему число. В полях определены операции сложения, вычитания, умножения и деления. При этом выражение $\boldsymbol{i} - \boldsymbol{j}$ следует понимать как $\boldsymbol{i} + (\boldsymbol{p} - \boldsymbol{j})$. Таким образом, можно считать, что в записи многочлена $f(x)$ нет слагаемых со знаком минус. Такой многочлен будем называть каноническим. Легко устанавливается следующий результат.

Пусть $f(x) = \boldsymbol{a_n} x^n + \boldsymbol{a_{n-1}} x^{n-1} + \cdots + \boldsymbol{a_1} x + \boldsymbol{a_0}$ *является каноническим многочленом над полем F_p. Элемент $\boldsymbol{i}$ является корнем многочлена $f(x)$ тогда и только*

тогда, когда соответствующее многочлену целое число $a_n i^n + a_{n-1} i^{n-1} + \cdots + a_1 i + a_0$ *делится на p.*

Таким образом, задача нахождения корней многочлена над полем F_p свелась к вычислению с целыми числами.

Проиллюстрируем сказанное на следующих примерах.

1. Найдем корни многочлена $f(x) = \mathbf{2}x^3 + x^2 + \mathbf{2}x + \mathbf{1}$ над полем F_3. Элементами поля являются **0**, **1**, **2**. Поэтому необходимо проверить делимость на 3 следующих чисел: $2 \cdot 0^3 + 0^2 + 2 \cdot 0 + 1 = 1$, $2 \cdot 1^3 + 1^2 + 2 \cdot 1 + 1 = 6$, $2 \cdot 2^3 + 2^2 + 2 \cdot 2 + 1 = 25$. Таким образом, многочлен имеет единственный корень, равный **1.**

2. Найдем корни многочлена $f(x) = \mathbf{2}x^3 + x^2 + \mathbf{2}x + \mathbf{2}$ над полем F_3. Необходимо проверить делимость на 3 следующих чисел: $2 \cdot 0^3 + 0^2 + 2 \cdot 0 + 2 = 2$, $2 \cdot 1^3 + 1^2 + 2 \cdot 1 + 2 = 7$, $2 \cdot 2^3 + 2^2 + 2 \cdot 2 + 2 = 26$. Так как ни одно из чисел не делится на 3, то многочлен не имеет корней.

Многочлен $f(x)$ над полем **P** называется неприводимым над этим полем, если его нельзя представить в виде произведения двух многочленов, степени которых не меньше единицы. Всякий многочлен является произведением неприводимых многочленов. Поэтому важна задача нахождения всех неприводимых многочленов степени n над конечным полем. Всякий многочлен, имеющий хотя бы один корень, не будет неприводимым. Поэтому быстрое нахождение корней многочлена играет важную роль в построении неприводимых многочленов.

Многочлен в примере 2 не имеет корней. Покажем, что он неприводим. Если бы $f(x)$ был приводим, то он должен быть равен произведению двух многочленов степеней не меньше единицы. Так как степень $f(x)$ равна 3, то один из сомножителей имеет степень, равную единице. Поэтому $f(x)$ должен иметь корень. Однако данный многочлен не имеет корней. Таким образом, $f(x)$ – неприводимый многочлен.

Случай быстрого нахождения корней многочлена над полем Галуа $GF(p^n)$, когда $n > 1$,значительно сложнее. Нами разработан алгоритм нахождения корней многочлена над полем $GF(2^2)$.

Список использованных источников

1. Лидл, Р. Конечные поля / Р. Лидл, Г. Нидеррайтер. – М. : Мир, 1988. – 714 с.