МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра Компьютерной алгебры и теории чисел

Конечные поля и операции над ними

АВТОРЕФЕРАТ БАКАЛАВРСКОЙ РАБОТЫ

студента 4 курса 421 группы

направления 02.03.01 Математика и компьютерные науки

механико-математического факультета

Коршунова Дмитрия Александровича

Научный руководитель

доцент, к.ф-м.н., доцент ____________ Крусс Ю.С.

подпись, дата

Зав. кафедрой

доцент, к.ф.-м.н., доцент ____________ А.М.Водолазов

подпись, дата

Саратов 2019

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра компьютерной алгебры и теории чисел

ОТЧЕТ ПО ПРОИЗВОДСТВЕННОЙ (ПРЕДДИПЛОМНОЙ) ПРАКТИКЕ

студентки 4 курса 421 группы

направления 02.03.01 Математика и компьютерные науки

механико-математического факультета

Коршунова Дмитрия Александровича

Место прохождения практики: кафедра КАиТЧ

Сроки прохождения практики: 06.02.2019 – 07.05.2019

Оценка:

Руководитель практики

к.ф.-м.н., доцент ______ Е.В. Сецинская

подпись, дата

Саратов 2019

Введение. С развитием информационных технологий и ростом электронного обмена информацией возникла потребность в защите данных от несанкционированного доступа, а также обеспечении их подлинности. В современной криптографии широко используется теория конечных полей.

Некоторые из алгоритмов, например шифр rijndael, основаны на сложении, умножении и делении многочленов. При этом используется арифметика конечного поля, отличающая от арифметики действительных чисел. Каждый элемент конечного поля может быть представлен в виде формального многочлена. Операция сложения определяется как сложение многочленов по модулю p. Результатом операции умножения является не произведение двух многочленов, а остаток от деления данного произведения на некоторый неприводимый многочлен. Данный многочлен выбирается и фиксируется. Выбирая разные неприводимые многочлены, мы будем получать разные результаты умножения.

Таким образом, для осуществления кодирования информации необходима программная реализация арифметики конечного поля.

Основное содержание работы. В первом разделе рассмотрим группы, кольца, поля.

Определение 1.1. Группой $(G, *)$ называется некоторое множество G с бинарной операцией $*$ на нём, для которые выполняются следующие условия:

1. Операция $*$ ассоциативна, т.е. для любых $a, b, c \in G$

$$(a * b) * c = a * (b * c).$$

2. В G существует единичный элемент (или единица) e, такой, что для любого $a \in G$

$$a * e = e * a = a.$$

3. Для каждого $a \in G$ существует обратный элемент $a^{-1} \in G$, такой, что

$$a * a^{-1} = a^{-1} * a = e.$$

Если группа удовлетворяет также следующему условию:

4. Для любых $a, b \in G$

$$a * b = b * a,$$

то она называется абелевой (или коммутативной).

Определение 1.2. Мультипликативная группа G называется циклической, если в ней имеется такой элемент a, что каждый элемент $b \in G$ является степенью элемента a, т.е. существует целое число k, такое, что $b = a^k$. Этот элемент a называется образующим группы G. Для циклической группы G применяют обозначения $G = (a)$.

Определение 1.3. Группа, образованная множеством $\{[0], [1], \ldots, [n-1]\}$ классов вычетов по модулю n с операцией

$$[a + b] = [a + b],$$

называется группой классов вычетов по модулю n и обозначается Z_n.

Определение 1.4. Группа называется конечной (бесконечной), если она состоит из конечного (бесконечного) числа элементов. Число элементов конечной группы называется ее порядком. Для порядка конечной группы G будем использовать обозначение $|G|$.

Существует удобный способ задания конечной группы - в виде таблицы, эта таблица, представляющая групповую операцию (обычно называется таблицей групповой операции или таблицей Кэли группы), строится так: её строки столбцы помечаются элементами группы и на пересечении строки, помеченной элементом a, и столбца, помеченного элементом b, становится элемент ab.

Пример 1.1. Таблица Кэли группы Z_6 имеет вид

+	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[1]	[2]	[3]	[4]	[5]
[1]	[1]	[2]	[3]	[4]	[5]	[0]
[2]	[2]	[3]	[4]	[5]	[0]	[1]
[3]	[3]	[4]	[5]	[0]	[1]	[2]
[4]	[4]	[5]	[0]	[1]	[2]	[3]
[5]	[5]	[0]	[1]	[2]	[3]	[4]

Определение 1.5. Отображение $f : G \to H$ группы G в группу H гомоморфизмом группы G в H, если оно сохраняет операцию группы G. Это значит, что если $*$ и $\cdot$ - операции в группах G и H соответственно, то для всех $a, b \in G$ имеет место равенство $f(a * b) = f(a) \cdot f(b)$. Если, кроме того, f - отображение на H, то оно называется эпиморфизмом (или гомоморфизмом «на»), и в этом случае H называется гомоморфным образом группы G. Гомоморфизм группы G в G называется эндоморфизмом этой группы. Если f - взаимно однозначный гомоморфизм группы G на группу H, то он называется изоморфизмом, и в таком случае говорят, что группы G и H изоморфны. Изоморфизм группы G на G называется автоморфизмом этой группы.

В качестве примера возьмем отображение f аддитивной группы Z целых чисел на группу Z_n классов вычетов по модулю n, определяемое условием $f(a) = [a]$. Тогда

$$f(a + b) = [a + b] = [a] + [b] = f(a) + f(b) \text{для} a, b \in Z,$$

так что f - гомоморфизм (точнее, эпиморфизм).

Если $f : G \to H$ - гомоморфизм и e - единичный элемент группы G, то из $ee = e$ следует $f(e)f(e) = f(e)$, так что $f(e) = e^{j}$ - единичный элемент груп- пы H. Из равенства $aa^{-1} = e$ получаем $f(a^{-1}) = (f(a))^{-1}$ для всех $a \in G$. Примером автоморфизмов группы G является ее внутренние автоморфизмы. Внутренний автоморфизм f_a определяется для фиксированного элемента a группы G условием $f_a(b) = aba^{-1}$ для всех $b \in G$. Очевидно, что f_a - авто- морфизм группы G, и все внутренние автоморфизмы группы G получаются, когда a пробегает все элементы группы G. Элементы b и aba^{-1} называют- ся сопряженными, и если S - непустое подмножество в G, то множество

$aSa^{-1} = \{asa^{-1} | s \in S\}$ называется сопряженным с S. Таким образом, сопряженными с S множествами в группе G оказываются образы множества S при всевозможных внутренних автоморфизмах группы G и только они.

Определение 1.6. Ядром гомоморфизма $f : G \to H$ группы G в группу H называется множество

$$Ker f = \{a \in G | f(a) = e'\},$$

где e' - единичный элемент группы H.

Определение 1.7. Кольцом (R, +, ·) 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

$$a \cdot (b + c) = a \cdot b + a \cdot c \qquad \text{и} \qquad (b + c) \cdot a = b \cdot a + c \cdot a$$

Определение 1.8.

1. 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 $a \in R$.

2. Кольцо называется коммутативным, если операция · коммутативна.

3. 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 $b = 0$.

4. Кольцо R называется телом, если $R \neq \{0\}$ и ненулевые элементы в R образуют группу относительно операции ·.

5. Коммутативное тело называется полем.

Прежде всего поле есть множество F, на котором заданы две операции, называемые сложением и умножением и которое содержит два выделенных элемента 0 и e, причем $0 \neq e$. 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 дистрибу- тивности $a(b + c) = ab + ac$. Второй закон дистрибутивности $(b + c)a = ba + ca$ выполняется автоматически с силу коммутативности умножения. Элемент 0 называется нулевым элементом (или нулем), а e - единичным элементом (или единицей) поля F.

Свойство, появляющиеся в определении (3): равенство $ab = 0$ влечет за собой $a = 0$ или $b = 0$. В частности, поле не имеет делителей нуля, так как если $ab = 0$ и $a \neq 0$, то умножение на a^{-1} дает $b = a^{-1}0 = 0$.

Пример 1.2. Приведем примеры к понятию кольца.

1. Пусть R - абелева группа с групповой операцией +. Определим умножение условием $ab = 0$ для всех $a, b \in R$. Тогда R становится кольцом.

2. Целые числа образуют целостное кольцо, но не поле.

3. Четные числа образуют коммутативное кольцо без единицы.

4. Функция $f : R \to R$ образуют коммутативное кольцо с единицей, если сумма $f + g$ и произведение fg определяются условиями $(f + g)(x) = f(x) + g(x)$ и $(fg)(x) = f(x)g(x)$ для любых $x \in R$.

5. Множество всех (2×2)-матриц с элементами из R образует некоммутативное кольцо с единицей относительно операций сложения и умножения матриц.

Поле, в частности, является целостным кольцом. Обратное, неверно, однако верно в случае, когда указанное целостное кольцо состоит из конечного числа элементов (т.е. является конечным кольцом).

Теорема 1.1. Каждое конечное целостное кольцо является полем.

Во втором разделе рассмотрим многочлены и неприводимые многочлены. Пусть R - произвольное кольцо. Многочленом (или полиномом) над R

называется выражение вида

$$f(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + \ldots + a_n x^n,$$

где n - неотрицательное целое число, коэффициенты a_i, $0 \le i \le n$ - элементы кольца R, а x - некоторый символ, не принадлежащий кольцу R, называемый переменной (или неизвестной) над R. Многочлены

$$f(x) = \sum_{i=0}^{n} a_i x^i \qquad \text{и} \qquad g(x) = \sum_{i=0}^{n} b_i x^i$$

над R считаются равными тогда и только тогда, когда $a_i = b_i$ для $0 \le i \le n$. Определим сумму многочленов $f(x)$ и $g(x)$ равенством

$$f(x) + g(x) = \sum_{i=0}^{n} (a_i + bi) x^i,$$

а произведение многочленов

$$f(x) = \sum_{i=0}^{m} a_i x^i \qquad \text{и} \qquad g(x) = \sum_{j=0}^{n} b_i x^j$$

равенством

$$f(x)g(x) = \sum_{k=0}^{m+n} c_k x_k, \qquad \text{где} \qquad c_k = \sum_{0 \le i \le m, 0 \le j \le n} a_i x_j$$

Определение 2.1. Кольцо, образованное многочленами над кольцом R с введенными выше операциями, называется кольцом многочленов над R и обозначается как $R[x]$.

Теорема 2.1. Пусть $g\ f = 0$ - многочлен из $F[x]$, где F - поле. Тогда для каждого $f\ s\ F[x]$ существует такие многочлены $q, r \in F[x]$, что

$$f = qg + r, \qquad \text{где} \qquad (r) < deg(g).$$

Определение 2.2. Многочлен $f \in F[x]$ называется неприводимым (неприводимым над полем F или в кольце $F[x]$), если он имеет положительную степень и равенство $f = gh, g, h$ s $F[x]$, может выполняться лишь в том случае, когда либо g, либо h является постоянным многочленом.

Многочлен положительной степени неприводим над F, если он допускает лишь тривиальное разложение на множители. Многочлен положительной степени из $F[x]$, не являющийся неприводимым над F, называется приводимым над F. Приводимость или неприводимость данного многочлена существенно зависит от того, над каким полем он рассматривается. Например, многочлен $x^2 - 2$ s $Q[x]$ неприводим над полем Q рациональных чисел, но приводим над полем R действительных чисел, так как $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$.

Неприводимые многочлены играют важную роль в устройстве кольца $F[x]$, поскольку каждый многочлен из $F[x]$ может быть записан и притом единственным способом в виде произведения неприводимых многочленов. Из этого выходит следующий результат.

Лемма 2.1. Если неприводимый многочлен f из $F[x]$ делит произведение $f_1 \dots f_m$ многочленов из $F[x]$, то по крайней мере один из сомножителей f_j делится на f.

Теорема 2.3. Элемент $b \in F$ является корнем многочлена $f \in F[x]$ в том и только том случае, когда многочлен $x - b$ делит f.

Теорема 2.4. Для неприводимости многочлена $f \in F[x]$ степени 2 или 3 в кольце $F[x]$ необходимо и достаточно, чтобы он не имел корней в поле F.

Определение 2.3. Поле, не содержащее собственных подполей, называется простым полем.

Любое поле порядка p при простом p - простое поле. Другим примером простого поля является поле Q рациональных чисел.

Пересечение любой непустой совокупности подполей данного поля F - снова подполе поля F. Пересечение всех подполей поля F называется простым подполе поля F. Очевидно, что оно является простым полем.

В третьем разделе рассмотрим конечные поля и представление элементов в виде многочленов.

Лемма 3.1. Пусть F - конечное поле, содержащее подполе K из q элементов. Тогда F состоит из q^m элементов, где $m = [F : K]$.

Теорема 3.1. Пусть F - конечное поле. Тогда оно состоит из p^n элементов, где простое число p является характеристикой поля F, а натуральное число n является степенью поля F над его простым подполем.

Лемма 3.2. Если F - конечное поле из q элементов, то каждый элемент $a \in F$ удовлетворяет равенству $a^q = a$.

Лемма 3.3. Если F - конечное поле из q элементов и K - подполе поля F, то многочлен $x^q - x$ из $K[x]$ вполне разлагается в $F[x]$ следующим образом:

$$x^q - x = \prod_{a \in F} (x - a),$$

так что F является полем разложения многочлена $x^q - x$ над полем K.

Теорема 3.2. (существование и единственность конечных полей). Для каждого простого числа p и каждого натурального числа n существует конечное поле из p^n элементов. Любое конечное поле из $q = p^n$ элементов изоморфно полю разложения многочлена $x^q - x$ над полем F_p.

Теорема 3.3.(критерий подполя). Пусть F_p - конечное поле из $q = p^n$ элементов (p - простое число). Тогда каждое подполе поля F_p имеет порядок p^m, где m является положительным делителем числа n. Обратно, если m - положительный делитель числа n, то существует ровно одно подполе поля F_q из p^m элементов.

Теорема 3.6. Если $f \in F_q[x]$ - неприводимый многочлен степени m, то в поле F_{q^m} содержится любой корень α многочлена f. Более того, все корни многочлена f просты и ими являются m различных элементов $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$ поля F_{q^m}.

Определение 3.4. Пусть K - поле характеристики p и n - натуральное число, не делящееся на p. Тогда образующий элемент циклической группы $E^{(n)}$ называется первообразным (или примитивным) корнем n-й степени из единицы над полем K.

Пример 3.2. Представим F_9 как простое алгебраическое расширение степени 2 поля F_3, получаемое присоединением $f(x) = x^2 + 1 \in F - 3[x]$. Тогда

$f(\alpha) = \alpha^2 + 1 = 0$ в F_9, и девять элементов поля F_9 можно задать в виде $a_0 + a_1\alpha$, где $a_0, a_1 \in F_3$. Точнее, $F_9 = \{0, 1, 2, \alpha, 1+\alpha, 2+\alpha, 2\alpha, 1+2\alpha, 2+2\alpha\}$.

Есть ещё один способ представления элементов поля F_q, этот способ представления дают применения теорем **??** и **??**. Поскольку поле F_q является $(q-1)$- круговым полем над F_p, мы можем построить его, найдя разложение $(q-1)$-кругового многочлена $Q_{q-1} \in F-p[x]$ на неприводимые сомножители в $F_p[x]$ (все они имеют одну и ту же степень). Любой корень каждого из этих многочленов тогда является первообразным корнем $(q-1)$-й степени из единицы над F_p, а значит, и примитивным элементом поля F_q. Таким образом, поле F_q состоит из нуля и степеней этого примитивного элемента.

В четвертом разделе содержится описание решения задачи построения алгебраического модуля для реализации алгебраических операций в конечном поле. В приложении приведен код программы, которая для заданных параметров p - характеристика поля, $f(x), g(x)$ осуществляет операции сложения, умножения и данных многочленов.

Заключение. В работе были приведены основные определения, касающихся конечных полей и неприводимых многочленов. Описан пример представления элементов конечного поля в виде многочлена. Для арифметики конечного поля написана программа на языке $C++$.