Вопросы для самоконтроля

1 Дать определение кольца. Привести примеры колец.

2 Что называется областью целостности?

3 Какое кольцо называется кольцом с единицей?

4 Что называется наибольшим общим делителем элементов кольца?

5 Что называется наименьшим общим кратным элементов кольца?

6 Дать определение операции деления с остатком в кольце.

7 Сформулировать расширенный алгоритм Евклида.

8 Как найти мультипликативный обратный элемент кольца вычетов?

9 Сформулировать алгоритм нахождения наибольшего общего делителя элементов кольца.

10 Дать определение символа Лежандра. Как найти символ Лежандра?

11 Как решить квадратичное сравнение по простому модулю?

2.4 Лабораторная работа 3. Поля. Конечные поля. Многочлены над простыми конечными полями. Арифметические операции в кольце многочленов над простым конечным полем

Цель работы: Повторить и реализовать основные алгоритмы теории полей, необходимые для решения задач алгебраической геометрии в криптографии.

Порядок выполнения лабораторной работы:

1. Повторить теоретические сведения, указанные в пункте 2.1.
2. Ознакомиться с примерами решения задач.
3. Выполнить и оформить задания лабораторной работы.
4. Подготовиться к защите работы.

Примеры решения задач

Задача 1. Найти корни многочлена $f(x) = x^7 + x^6 + x^5 + x^4 + x^2 + 1 \in F_2[x]$.

Решение.

Многочлен рассматривается над полем *GF(2)*. Корнями многочлена могут быть только элементы поля *GF(2)*, тот есть 0 и 1.

Найдем значения многочлена при $x = 0$ и $x = 1$.

$f(0) = 1 \neq 0 \Rightarrow x = 0$ не является корнем многочлена.

$f(1) = 0 (\mathrm{mod}\, 2) \Rightarrow x = 1$ является корнем многочлена.

Задача 2. Найдем корни многочлена $f(x) = x^3 + 2x^2 + 1 \in F_3[x]$. Является ли многочлен неприводимым?

Решение.

Многочлен рассматривается над полем *GF(3)*. Корнями многочлена могут быть только элементы поля *GF(3)*, то есть 0, 1 и 2.

Найдем значения многочлена при $x = 0$ и $x = 1$.

$f(0) = 1 \neq 0 \Rightarrow x = 0$ не является корнем многочлена.

$f(1) = 1 (\mathrm{mod}\, 3) \neq 0 \Rightarrow x = 1$ не является корнем многочлена.

$f(2) = 2^3 + 2 \cdot 2^2 + 1 = 2 (\mathrm{mod}\, 3) \neq 0 \Rightarrow x = 2$ не является корнем многочлена.

Таким образом, у многочлена корней нет.

Так как данный многочлен является многочленом степени 3 и не имеет корней, то он является неприводимым.

Задача 3. Используя схему Горнера, найти корни многочлена $f(x) = x^8 + x^7 + 4x^6 + 4x^5 + 3x^3 + 4x^2 + 3x + 2 \in F_5[x]$ и определить их кратность.

Решение.

Воспользуемся схемой Горнера, вычисления по которой представлены в таблице 3.

Таблица 3 – Схема Горнера для многочлена задачи 3

	1	1	4	4	0	3	4	3	2
0	1	1	4	4	0	3	4	3	$2 \neq 0$
1	1	2	1	0	0	3	2	0	$2 \neq 0$
2	1	3	0	4	3	4	2	2	$1 \neq 0$
3	1	4	1	2	1	1	2	4	4
4	1	0	4	0	0	3	1	2	0

Итак, корнем многочлена является $x_0 = 4$. Определим кратность корня. Многочлен $f(x) = (x-4)g(x)$, где $g(x) = x^7 + 4x^5 + 3x^2 + x + 2$. Корнями многочлена *g(x)* не могут быть элементы 0, 1, 2, 3. Выясним, является ли $x_0 = 4$ корнем *g(x)* (таблица 4).

Таблица 4 – Схема Горнера для многочлена $g(x) = x^7 + 4x^5 + 3x^2 + x + 2$

	1	0	4	0	0	3	1	2
4	1	4	0	0	0	3	3	$4 \neq 0$

Итак, $x_0 = 4$ корнем *g(x)* не является. Тогда корень $x_0 = 4$ многочлена *f(x)* имеет кратность 1.

Задача 4. Исследовать многочлен $f(x) = x^4 + x^2 + 1 \in F_2[x]$ на приводимость. Если многочлен приводимый, то разложить его на множители.

Решение.

Многочлен $f(x) = x^4 + x^2 + 1$ рассматривается над полем *GF(2)*. Корнями многочлена могут быть только элементы поля *GF(2)*, то есть 0 и 1.

Найдем значения многочлена при $x = 0$ и $x = 1$.

$f(0) = 1 \neq 0 \Rightarrow x = 0$ не является корнем многочлена.

$f(1) = 1 \neq 0 \Rightarrow x = 1$ не является корнем многочлена.

У многочлена нет корней. Таким образом, многочлен не может быть разложен на линейные множители.

Выясним, можно ли многочлен разложить на квадратичные множители.

Предположим, что $f(x) = x^4 + x^2 + 1 = (x^2 + ax + b)(x^2 + cx + d)$.

Тогда $x^4 + x^2 + 1 = x^4 + (a + c)x^3 + (ac + b + d)x^2 + (ad + bc)x + bd$.

Приравнивая коэффициенты при одинаковых степенях равных многочленов, получим систему над полем *GF(2)*

$$\begin{cases} a + c = 0, \\ ac + b + d = 1, \\ ad + bc = 0, \\ bd = 1. \end{cases} \tag{1.2}$$

Из последнего уравнения системы (1.2) получаем, что $b = d = 1$. Тогда первые три уравнения системы (1.2) примут следующий вид:

$$\begin{cases} a + c = 0, \\ ac = 1, \\ a + c = 0. \end{cases} \tag{1.3}$$

Из системы (1.3) получаем, что $a = c = 1$.

Таким образом, многочлен $f(x) = x^4 + x^2 + 1$ является приводимым и $f(x) = x^4 + x^2 + 1 = (x^2 + x + 1)(x^2 + x + 1)$.

Задача 5. Разделить многочлен $f(x) = 6x^5 + 2x^3 + 2x^2 + 3$ на многочлен $g(x) = 4x^3 + 2x^2 + 1$ над полем *GF(7)*.

Решение.

$$6x^5+0x^4+2x^3+2x^2+0x+3 \;\big|\; 4x^3+2x^2+1$$
$$\underline{6x^5+3x^4+\qquad 5x^2\qquad\qquad} \quad 5x^2+x$$
$$4x^4+2x^3+4x^2+0x+3$$
$$\underline{4x^4+2x^3+\qquad x\qquad} $$
$$4x^2+6x+3$$

Итак, частным от деления многочлена *f(x)* на многочлен *g(x)* является многочлен $h(x)=5x^2+x$, а остатком – многочлен $r(x)=4x^2+6x+3$.

Задача 6. Найти *НОД(f(x),g(x))* и его линейное представление, если $f(x)=x^5+x^2+1,\ g(x)=x^4+x+1$ – многочлены над полем *GF(2)*.

Решение.

Воспользуемся расширенным алгоритмом Евклида для многочленов. Вычисления оформим в таблице 5.

Таблица 5 – Поиск $НОД(x^5+x^2+1, x^4+x+1)$ и его линейного представления

i	a_i	x_i	y_i	q_i
0	x^5+x^2+1	1	0	–
1	x^4+x+1	0	1	x
2	$x+1$	1	$-x$	x^3+x^2+x
3	1	x^3+x^2+x	$x^4+x^3+x^2+1$	$x+1$
4	0			

Итак,

$$НОД(x^5+x^2+1, x^4+x+1)=1=$$
$$=(x^5+x^2+1)(x^3+x^2+x)+(x^4+x+1)(x^4+x^3+x^2+1).$$

Задача 7. Пусть $f(x)=2x^2+1,\ \ g(x)=x^4+x+2$ – многочлены из кольца $F_3[x]$. Найти $f(x)^{-1}(\mathrm{mod}\, g(x))$.

Решение.

Для нахождения $f(x)^{-1}(\mathrm{mod}\, g(x))$ воспользуемся расширенным алгоритмом Евклида для многочленов, вычисления по которому представлены в таблице 6.

Таблица 6 – Поиск $НОД(2x^2+1, x^4+x+2)$ и его линейного представления

i	a_i	x_i	y_i	q_i
0	x^4+x+2	1	0	–
1	$2x^2+1$	0	1	$2x^2+2$
2	x	1	x^2+1	$2x$
4	1	x	x^3+x+1	x
5	0			

Так как $НОД(2x^2+1, x^4+x+2)=1=(2x^2+1)(x^3+x+1)+(x^4+x+2)\cdot x$, то $f(x)^{-1}(\mathrm{mod}\, g(x))=x^3+x+1.$

Задания лабораторной работы

Для заданий лабораторной работы N – номер варианта, который указывается преподавателем, остальные значения находятся по следующим правилам:

$a_i = i+N(\mathrm{mod}\,2)$, $i=\overline{0,8}$, $b_j = j+N(\mathrm{mod}\,7)$, $j=\overline{0,6}$,

$c_k = k+N(\mathrm{mod}\,3)$, $k=\overline{0,4}$, $d_l = l+N(\mathrm{mod}\,5)$, $l=\overline{0,3}$,

$r_m = m+N(\mathrm{mod}\,11)$, $m=\overline{0,7}$, $s_t = t+N(\mathrm{mod}\,11)$, $t=\overline{0,3}$.

1. Найти корни многочленов:

а) $f(x)=x^9+a_8x^8+a_7x^7+a_6x^6+a_5x^5+a_4x^4+a_3x^3+a_2x^2+a_1x+a_0\in F_2[x]$;

б) $f(x)=b_6x^6+b_5x^5+b_4x^4+b_3x^3+b_2x^2+b_1x+b_0\in F_7[x]$.

2. Исследовать многочлены на приводимость. Приводимые многочлены разложить на множители.

а) $f(x)=x^5+c_4x^4+c_3x^3+c_2x^2+c_1x+c_0\in F_3[x]$;

б) $f(x) = x^4 + d_3x^3 + d_2x^2 + d_1x + d_0 \in F_5[x]$.

3. Найти *НОД(f(x),g(x))* и его линейное представление, если $f(x) = r_7x^7 + r_6x^6 + r_5x^5 + r_4x^4 + r_3x^3 + r_2x^2 + r_1x + r_0$ и $g(x) = s_3x^3 + s_2x^2 + s_1x + s_0$ – многочлены над полем *GF*(11).

4. Пусть $f(x) = s_2x^2 + s_1x + s_0$, $g(x) = x^8 + x^4 + x^3 + 6x + 2$ – многочлены над полем *GF*(13). Найти $f(x)^{-1}(\mathrm{mod}\, g(x))$.

5. Реализовать арифметические операции над многочленами над простыми конечными полями, алгоритмы генерации неприводимых многочленов над простыми конечными полями.

Вопросы для самоконтроля

1 Дать определения поля. Привести примеры.

2 Что называется подполем?

3 Какое поле называется простым? Привести примеры простых полей.

4 Что называется порядком поля?

5 Какое поле называется конечным? Чему равен порядок конечного поля?

6 Чему равен порядок мультипликативной группы конечного поля?

7 Какое конечное поле является простейшим?

8 Какие поля составляют класс всех простых конечных полей?

9 Какие поля называются изоморфными?

10 Что называется многочленом над полем? Что называется степенью многочлена? Какой многочлен называется нормированным?

11 Каким образом определяются операции сложения и умножения многочленов?

12 Каким образом в кольце многочленов определяется операция деления с остатком?

13 Как найти наибольший общий делитель двух многочленов?

2.5 Лабораторная работа 4. Построение полей Галуа

Цель работы: Реализовать построение полей Галуа.

Порядок выполнения лабораторной работы:

1. Повторить теоретические сведения, указанные в пункте 2.1.
2. Ознакомиться с примерами решения задач.
3. Выполнить и оформить задания лабораторной работы.
4. Подготовиться к защите работы.

Примеры решения задач

Задача 1. Построить конечное поле $GF(3)$ и его расширение $GF(3^2)$. Найти примитивный элемент поля $GF(3^2)$. Записать различные представления элементов поля $GF(3^2)$ (многочлен, вектор, степень).

Решение.

Пусть элементами множества $GF(3)$ являются 0, 1 и 2. Определим операции над элементами в $GF(3)$. Свойства конечного поля в $GF(3)$ будут выполняться, если в качестве операций сложения и умножения использовать операции по модулю 3.

В таблицах 6 и 7 заданы операции сложения и умножения элементов поля $GF(3)$.

Таблица 6 – Таблица сложения элементов поля $GF(3)$

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Таблица 7 – Таблица умножения элементов поля $GF(3)$

×	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Построим поле $GF(3^2)$ как факторкольцо $F_3[x]/(f(x))$, где $f(x)$ – неприводимый многочлен над полем $GF(3)$.

Находим неприводимый многочлен второй степени над $GF(3)$. Например, $f(x)=x^2+x+2$. Множество $F_3[x]/(f(x))$ состоит из 9 элементов, которые являются классами вычетов. Обозначим классы вычетов следующим образом: 0, 1, 2, α, $\alpha+1$, $\alpha+2$, 2α, $2\alpha+1$, $2\alpha+2$ (причем α является корнем многочлена $f(x)=x^2+x+2$).

В таблицах 8 и 9 заданы операции сложения и умножения элементов поля $GF(3^2)$.

Таблица умножения в $GF(3^2)$ определяется из соотношения $\alpha^2=2\alpha+1$.

Различные представления элементов поля $GF(3^2)$ (многочлен, вектор, степень) представлены в таблице 10.

Таблица 8 – Таблица сложения элементов поля $GF(3^2)$

+	0	1	2	α	$\alpha+1$	$\alpha+2$	2α	$2\alpha+1$	$2\alpha+2$
0	0	1	2	α	$\alpha+1$	$\alpha+2$	2α	$2\alpha+1$	$2\alpha+2$
1	1	2	0	$\alpha+1$	$\alpha+2$	α	$2\alpha+1$	$2\alpha+2$	2α
2	2	0	1	$\alpha+2$	α	$\alpha+1$	$2\alpha+2$	2α	$2\alpha+1$
α	α	$\alpha+1$	$\alpha+2$	2α	$2\alpha+1$	$2\alpha+2$	0	1	2
$\alpha+1$	$\alpha+1$	$\alpha+2$	α	$2\alpha+1$	$2\alpha+2$	2α	1	2	0
$\alpha+2$	$\alpha+2$	α	$\alpha+1$	$2\alpha+2$	2α	$2\alpha+1$	2	0	1
2α	2α	$2\alpha+1$	$2\alpha+2$	0	1	2	α	$\alpha+1$	$\alpha+2$
$2\alpha+1$	$2\alpha+1$	$2\alpha+2$	2α	1	2	0	$\alpha+1$	$\alpha+2$	α
$2\alpha+2$	$2\alpha+2$	2α	$2\alpha+1$	2	0	1	$\alpha+2$	α	$\alpha+1$

Таблица 9 – Таблица умножения элементов поля $GF(3^2)$

$\times$	0	1	2	α	$\alpha+1$	$\alpha+2$	2α	$2\alpha+1$	$2\alpha+2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	α	$\alpha+1$	$\alpha+2$	2α	$2\alpha+1$	$2\alpha+2$
2	0	2	1	2α	$2\alpha+2$	$2\alpha+1$	α	$\alpha+2$	$\alpha+1$
α	0	α	2α	$2\alpha+1$	1	$\alpha+1$	$\alpha+2$	$2\alpha+2$	2
$\alpha+1$	0	$\alpha+1$	$2\alpha+2$	1	$\alpha+2$	2α	2	α	$2\alpha+1$
$\alpha+2$	0	$\alpha+2$	$2\alpha+1$	$\alpha+1$	2α	2	$2\alpha+2$	1	α
2α	0	2α	α	$\alpha+2$	2	$2\alpha+2$	$2\alpha+1$	$\alpha+1$	1
$2\alpha+1$	0	$2\alpha+1$	$\alpha+2$	$2\alpha+2$	α	1	$\alpha+1$	2	2α
$2\alpha+2$	0	$2\alpha+2$	$\alpha+1$	2	$2\alpha+1$	α	1	2α	$\alpha+2$

Таблица 10 – Различные представления элементов поля $GF(3^2)$

Многочлен	Степень α	Вектор (a_0, a_1)
1	α^0	(1, 0)
α	α^1	(0, 1)
$2\alpha+1$	α^2	(1, 2)
$2\alpha+2$	α^3	(2, 2)
2	α^4	(2, 0)
2α	α^5	(0, 2)
$\alpha+2$	α^6	(2, 1)
$\alpha+1$	α^7	(1, 1)

Задания лабораторной работы

Для заданий лабораторной работы N – номер варианта, который указывается преподавателем.

1. Построить конечное поле $GF(p)$ и его расширение $GF(p^m)$. Найти примитивный элемент поля $GF(p^m)$. Записать различные представления элементов поля $GF(p^m)$ (многочлен, вектор, степень), если известно, что

$$p=\begin{cases}5, N\equiv 0(\mathrm{mod}\,5),\\ 3, N\equiv 1(\mathrm{mod}\,5),\\ 2, N\equiv 2(\mathrm{mod}\,5),\\ 13, N\equiv 3(\mathrm{mod}\,5),\\ 11, N\equiv 4(\mathrm{mod}\,5),\end{cases} \quad m=\begin{cases}3, N\equiv 0(\mathrm{mod}\,5),\\ 4, N\equiv 1(\mathrm{mod}\,5),\\ 7, N\equiv 2(\mathrm{mod}\,5),\\ 2, N\equiv 3(\mathrm{mod}\,5),\\ 2, N\equiv 4(\mathrm{mod}\,5).\end{cases}$$

2. Написать программу, реализующую построение конечных полей.

Вопросы для самоконтроля

1 Перечислить свойства мультипликативной группы конечного поля.

2 Какой элемент циклической группы называется примитивным элементом конечного поля?

3 Перечислить свойства характеристики поля, конечного поля?

4 Дать определение простого расширения поля.

5 Какой многочлен называется неприводимым над полем?

6 Что называется простым алгебраическим расширением поля степени n?

7 Дать определение конечного расширения поля. Что называется базисом поля? Что называется степенью конечного расширения поля?

8 Какое поле называется полем разложения многочлена?

9 Какой многочлен называется минимальным многочленом элемента поля?

10 Какой многочлен называется примитивным?