Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Оренбургский государственный университет»

Кафедра алгебры и дискретной математики

О.А. Пихтилькова, А.Н. Благовисная

ЛАБОРАТОРНЫЕ РАБОТЫ ПО ДИСЦИПЛИНЕ «МЕТОДЫ АЛГЕБРАИЧЕСКОЙ ГЕОМЕТРИИ В КРИПТОГРАФИИ»

Методические указания

Рекомендовано к изданию редакционно-издательским советом федерального государственного бюджетного образовательного учреждения высшего образования «Оренбургский государственный университет» для обучающихся по образовательной программе высшего образования по направлению подготовки 02.03.01 Математика и компьютерные науки

Оренбург
2019

УДК 004.056.55:512.7(076.5)
ББК 22.147я7+32.972.5я7
П 35

Рецензент – доцент, кандидат физико-математических наук С.А. Герасименко

Пихтилькова, О.А.

П 35 Лабораторные работы по дисциплине «Методы алгебраической геометрии в криптографии»: методические указания / О.А. Пихтилькова, А.Н. Благовисная; Оренбургский гос. ун-т. – Оренбург: ОГУ, 2019. – 77 с.

Методические указания содержат рекомендации по выполнению лабораторных работ по дисциплине «Методы алгебраической геометрии в криптографии».

Методические указания предназначены для обучающихся по направлению подготовки 02.03.01 Математика и компьютерные науки.

УДК 004.056.55:512.7(076.5)
ББК 22.147я7+32.972.5я7

Содержание

Введение

Настоящие методические указания предназначены для проведения лабораторных работ по дисциплине «Методы алгебраической геометрии в криптографии» для обучающихся по направлению подготовки 02.03.01 Математика и компьютерные науки.

Содержание разделов методических указаний соответствует рабочей программе дисциплины «Методы алгебраической геометрии в криптографии» и включает в себя необходимые для успешного освоения дисциплины составляющие: теоретические сведения, необходимые для выполнения лабораторных работ, примеры решения задач, вопросы для самоконтроля.

Материалы методических указаний составлены на основе литературы, указанной в списке использованных источников.

1 Рекомендации по оформлению лабораторных работ

К лабораторным работам предъявляется ряд требований, основным из которых является полное, исчерпывающее описание всей проделанной работы, позволяющее судить о полученных результатах, степени выполнения заданий и профессиональной подготовке обучающихся. Лабораторная работа оформляется как небольшой отчет, отражающий всю работу, проведенную обучающимся.

Отчет по лабораторной работе оформляется индивидуально каждым обучающимся в соответствии с «СТО 02069024.101–2015 РАБОТЫ СТУДЕНЧЕСКИЕ. Общие требования и правила оформления». Стандарт можно найти на официальном сайте Оренбургского государственного университета по ссылке http://www.osu.ru/docs/official/standart/standart_101-2015_.pdf.

2 Основы и алгоритмы теории групп, колец и полей, необходимые для реализации методов алгебраической геометрии в криптографии

2.1 Основные теоретические сведения, необходимые для выполнения лабораторных работ

Основные теоретические сведения, необходимые для выполнения заданий лабораторных работ данного раздела, можно найти в [3] (см. список использованных источников). Перед выполнением заданий лабораторных работ рекомендуется повторить следующие разделы алгебры:

1) группы [3, с. 6-15];

2) кольца и поля [3, с. 16-20];

3) кольца и поля вычетов [3, с. 37-40];

4) элементы теории многочленов [3, с. 41-51];

5) элементы теории полей [3, с. 52-59].

2.2 Лабораторная работа 1. Группы. Поиск порядка элемента группы, образующего элемента группы. Построение смежных классов

Цель работы: Повторить и реализовать основные алгоритмы теории групп, 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 подгруппы аддитивной группы Z_{12}. Построить смежные классы по собственным подгруппам. Чему равен индекс группы по каждой из подгрупп?

Решение.

Подгруппами аддитивной абелевой группы Z_{12} будут следующие множества: $H_0 = \{\bar{0}\}$, $H_1 = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \overline{10}\}$, $H_2 = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}\}$, $H_3 = \{\bar{0}, \bar{4}, \bar{8}\}$, $H_4 = \{\bar{0}, \bar{6}\}$ и $H_5 = Z_{12} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}, \bar{9}, \overline{10}, \overline{11}\}$.

Собственными подгруппами являются: $H_1 = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \overline{10}\}$, $H_2 = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}\}$, $H_3 = \{\bar{0}, \bar{4}, \bar{8}\}$, $H_4 = \{\bar{0}, \bar{6}\}$.

Смежными классами по подгруппе H_1 являются множества: $\{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \overline{10}\}$, $\{\bar{1}, \bar{3}, \bar{5}, \bar{7}, \bar{9}, \overline{11}\}$. Индекс группы Z_{12} по подгруппе H_1 равен количеству смежных классов, то есть 2.

Смежными классами по подгруппе H_2 являются множества: $\{\bar{0}, \bar{3}, \bar{6}, \bar{9}\}$, $\{\bar{1}, \bar{4}, \bar{7}, \overline{10}\}$, $\{\bar{2}, \bar{5}, \bar{8}, \overline{11}\}$. Индекс группы Z_{12} по подгруппе H_2 равен 3.

Смежными классами по подгруппе H_3 являются множества: $\{\bar{0}, \bar{4}, \bar{8}\}$, $\{\bar{1}, \bar{5}, \bar{9}\}$, $\{\bar{2}, \bar{6}, \overline{10}\}$, $\{\bar{3}, \bar{7}, \overline{11}\}$. Индекс группы Z_{12} по подгруппе H_3 равен 4.

Смежными классами по подгруппе H_4 являются множества: $\{\bar{0}, \bar{6}\}$, $\{\bar{1}, \bar{7}\}$, $\{\bar{2}, \bar{8}\}$, $\{\bar{3}, \bar{9}\}$, $\{\bar{4}, \overline{10}\}$, $\{\bar{5}, \overline{11}\}$. Индекс группы Z_{12} по подгруппе H_4 равен 6.

Задача 2. Найти все подгруппы мультипликативной группы Z_{15}^*.

Решение.

Выпишем элементы группы Z_{15}^*: $\bar{1}, \bar{2}, \bar{4}, \bar{7}, \bar{8}, \overline{11}, \overline{13}, \overline{14}$.

Подгруппами группы Z_{15}^* будут следующие множества: $H_0 = \{\bar{1}\}$, $H_1 = \{\bar{1}, \bar{2}, \bar{4}, \bar{8}\}$, $H_2 = \{\bar{1}, \bar{4}\}$, $H_3 = \{\bar{1}, \bar{4}, \bar{7}, \overline{13}\}$, $H_4 = \{\bar{1}, \overline{14}\}$, $H_5 = \{\bar{1}, \bar{2}, \bar{4}, \bar{7}, \bar{8}, \overline{11}, \overline{13}, \overline{14}\}$.

Задача 3. Вычислить $\varphi(1200)$.

Решение.

Найдем каноническое разложение числа $1200 = 2^4 \cdot 3 \cdot 5^2$.

$$\varphi(2^4 \cdot 3 \cdot 5^2) = 2^4 \cdot 3 \cdot 5^2 \cdot \left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right) = 320.$$

Задача 4. Пусть $G = \{e, g, g^2, ..., g^{11}\}$, $g^{12} = e$ – циклическая группа порядка 12. Найти порядки элементов g^6, g^8, g^9 группы G и выписать элементы порожденных ими циклических подгрупп.

Решение.

Наименьшее натуральное n, для которого $(g^6)^n = e = g^{12}$, равно 2, то есть порядок элемента $ordg^6 = 2$. Элемент g^6 порождает подгруппу $H = \{e, g^6\}$.

Известно, что порядок элемента $ordg^k = \dfrac{ordg}{НОД(k, ordg)}$. Так как $ordg = 12$, $НОД(k, ordg) = НОД(8,12) = 4$, то $ordg^8 = \dfrac{12}{4} = 3$. Элемент g^8 порождает подгруппу $H = \{e, g^4, g^8\}$.

$ordg^9 = \dfrac{12}{НОД(9,12)} = 4$. Элемент g^9 порождает подгруппу $H = \{e, g^3, g^6, g^9\}$.

Задача 5. В циклической группе порядка 18 найти все элементы g такие, что $g^3 = e$ и все элементы порядка 3.

Решение.

Пусть $G = \langle g \rangle = \{e, g, g^2, ..., g^{17}\}$. Имеем $\left(g^k\right)^3 = e \Leftrightarrow 18 \mid 3k$ или $6 \mid k$, то есть $k = 0, 6, 12$. Таким образом, элементами, пятая степень которых равна единичному элементу, являются e, g^6, g^{12}.

Так как $ordg^k = \dfrac{ordg}{НОД(k, ordg)} = \dfrac{18}{НОД(k,18)}$, то $ordg^k = 3 \Leftrightarrow \dfrac{18}{НОД(k,18)} = 3$ или $НОД(k,18) = 6$. Тогда $k = 6, 12$ и элементами третьего порядка являются элементы g^6, g^{12}.

Задача 6. Пусть 10 – элемент мультипликативной группы кольца вычетов по модулю 23. Найти 10^{25}.

Решение.

По малой теореме Ферма $10^{22} \equiv 1(\mathrm{mod}\,23)$. Тогда $10^{25} \equiv 10^3 \equiv 11(\mathrm{mod}\,23)$.

Задача 7. Найти порядок элемента 15 в мультипликативной группе кольца вычетов по модулю 41. Является ли элемент 15 образующим элементом мультипликативной группы кольца вычетов по модулю 41?

Решение.

По малой теореме Ферма $15^{40} \equiv 1(\mathrm{mod}\,41)$. Найдем $15^{20} \equiv -1(\mathrm{mod}\,41)$. Тогда $ord 15 = 40$. Мультипликативная группа кольца вычетов по модулю 41 является циклической и её порядок равен 40 и равен порядку элемента 15, поэтому 15 является образующим элементом группы.

Задача 8. Найти все образующие элементы аддитивной группы вычетов по модулю 30.

Решение.

Количество образующих элементов группы равно $\varphi(30) = \varphi(2 \cdot 3 \cdot 5) = \varphi(2)\varphi(3)\varphi(5) = 1 \cdot 2 \cdot 4 = 8$. Так как $Z_{30} = \langle \bar{1} \rangle$, то $\bar{s} = s\bar{1}$ является образующим тогда и только тогда, когда $НОД(s, 30) = 1$. То есть образующими являются $\bar{1}, \bar{7}, \overline{11}, \overline{13}, \overline{17}, \overline{19}, \overline{23}, \overline{29}$.

Задача 9. Найти в группе Z_{30} циклическую подгруппу, порожденную элементом $\overline{25}$.

Решение.

Так как $\overline{25} \cdot 1 = \overline{25}$, $\overline{25} \cdot 2 = \overline{20}$, $\overline{25} \cdot 3 = \overline{15}$, $\overline{25} \cdot 4 = \overline{10}$, $\overline{25} \cdot 5 = \bar{5}$, $\overline{25} \cdot 6 = \bar{0}$, то в группе Z_{30} циклическая подгруппа, порожденная элементом $\overline{25}$, имеет вид $H = \{\bar{0}, \bar{5}, \overline{10}, \overline{15}, \overline{20}, \overline{25}\}$.

Задача 10. Найти в группе Z_{14}^* циклическую подгруппу, порожденную элементом $\bar{5}$.

Решение.

Так как $\left(\bar{5}\right)^1=\bar{5}$, $\left(\bar{5}\right)^2=\overline{11}$, $\left(\bar{5}\right)^3=\overline{13}$, $\left(\bar{5}\right)^4=\bar{9}$, $\left(\bar{5}\right)^5=\bar{3}$, $\left(\bar{5}\right)^6=\bar{1}$, то в группе Z_{14}^* циклическая подгруппа, порожденная элементом $\bar{5}$, имеет вид $H=\left\{\bar{1},\bar{3},\bar{5},\bar{9},\overline{11},\overline{13}\right\}$.

Задания лабораторной работы

Для заданий лабораторной работы N – номер варианта, который указывается преподавателем. Значения m, n, n_1, n_2, n_3, k, p, s, r, t находятся по следующим правилам:

$$m=\begin{cases}15(N+2), N<10,\\ 12(N-4), N>10,\end{cases}\quad n=\begin{cases}5(N+1), N<10,\\ 3(N-5), N>10,\end{cases}$$

$$n_1=\begin{cases}N, N<10,\\ N-7, N>10,\end{cases}\quad n_2=\begin{cases}N+2, N<10,\\ N-5, N>10,\end{cases}\quad n_3=\begin{cases}N+4, N<10,\\ N-4, N>10,\end{cases}$$

$$k=\begin{cases}N+2, N<10,\\ N-2, N>10,\end{cases}$$

$$p=\begin{cases}29, N\equiv 0(\mathrm{mod}\,5),\\ 31, N\equiv 1(\mathrm{mod}\,5),\\ 37, N\equiv 2(\mathrm{mod}\,5),\\ 23, N\equiv 3(\mathrm{mod}\,5),\\ 19, N\equiv 4(\mathrm{mod}\,5),\end{cases}\quad s=\begin{cases}5, N\equiv 0(\mathrm{mod}\,5),\\ 4, N\equiv 1(\mathrm{mod}\,5),\\ 3, N\equiv 2(\mathrm{mod}\,5),\\ 17, N\equiv 3(\mathrm{mod}\,5),\\ 15, N\equiv 4(\mathrm{mod}\,5),\end{cases}\quad r=\begin{cases}59, N\equiv 0(\mathrm{mod}\,5),\\ 60, N\equiv 1(\mathrm{mod}\,5),\\ 38, N\equiv 2(\mathrm{mod}\,5),\\ 45, N\equiv 3(\mathrm{mod}\,5),\\ 44, N\equiv 4(\mathrm{mod}\,5),\end{cases}$$

$$t=\begin{cases}9, N\equiv 0(\mathrm{mod}\,5),\\ 8, N\equiv 1(\mathrm{mod}\,5),\\ 7, N\equiv 2(\mathrm{mod}\,5),\\ 12, N\equiv 3(\mathrm{mod}\,5),\\ 14, N\equiv 4(\mathrm{mod}\,5).\end{cases}$$

1. Найти подгруппы аддитивной группы Z_m. Построить смежные классы по одной из собственных подгрупп. Чему равен индекс группы по каждой из собственных подгрупп?

2. Найти все подгруппы мультипликативной группы Z_m^*.

3. Вычислить $\varphi(60N+15)$.

4. Пусть $G=\{e,g,g^2,...,a^{n-1}\}, g^n=e$ – циклическая группа порядка n. Найти порядки элементов g^{n_1}, g^{n_2}, g^{n_3} группы G и выписать элементы порожденных ими циклических подгрупп.

5. В циклической группе порядка m найти все элементы g такие, что $g^k=e$ и все элементы порядка k.

6. Пусть s – элемент мультипликативной группы Z_p^*. Найти s^r.

7. Найти порядок элемента t в группе вычетов по модулю p. Является ли элемент t образующим элементом мультипликативной группы кольца вычетов по модулю p?

8. Найти все образующие элементы аддитивной группы вычетов по модулю m.

9. Найти в группе Z_m циклическую подгруппу, порожденную элементом t.

10. Найти в группе Z_m^* циклическую подгруппу, порожденную элементом s.

11. Написать программы, реализующие поиск порядка элемента группы, образующего элемента группы, построение смежных классов.

Вопросы для самоконтроля

1 Дать определение группы. Какой элемент группы называется нейтральным (единичным)? Какой элемент группы называется симметричным? Дать определение операции инверсии.

2 Какая группа называется абелевой? Привести примеры абелевых групп.

3 Какая группа называется аддитивной? Как обозначают бинарную операцию аддитивной группы? Как называется нейтральный элемент аддитивной группы? Как называется результат операции аддитивной инверсии?

4 Какая группа называется мультипликативной? Как обозначают бинарную операцию мультипликативной группы? Как называется нейтральный элемент мультипликативной группы? Как называется результат операции мультипликативной инверсии?

5 Что называется k-й степенью элемента группы?

6 Что называется операцией вычитания элемента b из элемента a в аддитивной группе? Что называется разностью элементов a и b?

7 Что называется операцией деления элемента a на элемент b в мультипликативной группе? Что называется частным от деления элемента a на элемент b?

8 Какая группа называется конечной?

9 Привести примеры тривиальных аддитивной и мультипликативной групп.

10 Привести примеры простейших нетривиальных конечных аддитивной и мультипликативной групп.

11 Что называется порядком конечной группы?

12 Что называется порядком элемента группы?

13 Какой элемент называется образующим элементом группы?

14 Какая группа называется циклической?

15 Как определяется на множестве целых чисел отношение эквивалентности по модулю m? Как обозначается фактор-множество по этому отношению?

16 Каким образом на Z_m определяются операции сложения и умножения?

17 Показать, что Z_m является абелевой группой.

18 Какие элементы Z_m образуют мультипликативную группу?

19 Дать определение подгруппы.

20 Дать определение левых смежных классов по подгруппе. Чему равно число элементов в каждом классе?

21 Что называется индексом подгруппы в группе?

22 Сформулировать теорему Лагранжа.

23 Дать определение правых смежных классов по подгруппе. В какой группе левые и правые смежные классы совпадают?

24 Сформулировать следствия теоремы Лагранжа.

25 Сформулировать теорему Эйлера.

26 Сформулировать теорему Лагранжа.

27 Сформулировать алгоритм возведения в степень элемента мультипликативной группы.

28 Как найти образующий элемент циклической группы?

2.3 Лабораторная работа 2. Кольца. Арифметические операции в кольцах вычетов по модулю *m*

Цель работы: Повторить и реализовать основные алгоритмы теории колец, 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 *НОД(1628,4678)* и коэффициенты его линейного разложения.

Решение.

Воспользуемся расширенным алгоритмом Евклида. Вычисления оформим в таблице 1.

Таблица 1 – Поиск *НОД(1628,4678)* и его линейного представления

i	a_i	x_i	y_i	q_i
0	4678	1	0	–
1	1628	0	1	2
2	1422	1	– 2	1
3	206	– 1	3	6
4	186	7	– 20	1
5	20	– 8	23	9
6	6	79	– 227	3
7	2	– 245	704	3
8	0			

Итак, $НОД(1628,4678) = 2 = 1628 \cdot 704 + 4678 \cdot (-245)$.

Задача 2. Найти $28^{-1}(\mathrm{mod}167)$.

Решение.

Для нахождения $28^{-1}(\mathrm{mod}167)$ воспользуемся расширенным алгоритмом Евклида, вычисления согласно которому представлены в таблице 2.

Таблица 2 – Поиск *НОД(28,167)* и его линейного представления

i	a_i	x_i	y_i	q_i
0	167	1	0	–
1	28	0	1	5
2	27	1	– 5	1
3	1	– 1	6	27
4	0			

Так как $НОД(28,167) = 1 = 28 \cdot 6 + 167 \cdot (-1)$, то $28^{-1}(\mathrm{mod}167) = 6$.

Задача 3. Найти символ Лежандра $\left(\frac{188}{263}\right)$.

Решение.

Найдем символ Лежандра, используя его свойства (приложение А):

$$\left(\frac{188}{263}\right)=\left(\frac{2^2\cdot 47}{263}\right)=\left|свойство\ 3\right|=\left(\frac{47}{263}\right)=\left|свойство\ 7\right|=(-1)^{\frac{47-1}{2}\cdot\frac{263-1}{2}}\left(\frac{263}{47}\right)=$$

$$=|\,свойство\ 1|=-\left(\frac{28}{47}\right)=-\left(\frac{2^2\cdot 7}{47}\right)=|\,свойство\ 3|=-\left(\frac{7}{47}\right)=|\,свойство\ 7\,|=$$

$$=-(-1)^{\frac{7-1}{2}\cdot\frac{47-1}{2}}\left(\frac{47}{7}\right)=|\,свойство\ 1|=\left(\frac{5}{7}\right)=|\,свойство\ 7\,|=(-1)^{\frac{5-1}{2}\cdot\frac{7-1}{2}}\left(\frac{7}{5}\right)=.$$

$$=|\,свойство\ 1|=\left(\frac{2}{5}\right)=|\,свойство\ 6\,|=-1.$$

Задача 4. Решить квадратичное сравнение $x^2\equiv 62(\mathrm{mod}\,97)$.

Решение.

Решим сравнение

$$x^2\equiv 62(\mathrm{mod}\,97). \qquad (1.1)$$

Модуль сравнения (1.1) равен 97 и является простым числом. Выясним, имеет ли сравнение (1.1) решения. Для того чтобы определить, есть ли решения у сравнения, найдем символ Лежандра:

$$\left(\frac{62}{97}\right)=\left(\frac{2\cdot 31}{97}\right)=|\,свойство\ 3|=\left(\frac{2}{97}\right)\left(\frac{31}{97}\right)=\left|\begin{matrix}свойство\ 6,\\ свойство\ 7\end{matrix}\right|=$$

$$=(-1)^{\frac{97^2-1}{8}}\cdot(-1)^{\frac{31-1}{2}\cdot\frac{97-1}{2}}\left(\frac{97}{31}\right)=\left(\frac{97}{31}\right)=|\,свойство\ 1|=\left(\frac{4}{31}\right)=\left(\frac{2^2}{31}\right)=\left(\frac{2}{31}\right)^2=1.$$

Так как символ Лежандра $\left(\frac{62}{97}\right)$ равен 1, то число 62 является вычетом по модулю 97 и сравнение (1.1) имеет решения.

Буем искать решения сравнения (1.1), используя алгоритм Шенкса.

Напомним последовательность действий алгоритма Шенкса поиска решения сравнения $x^2\equiv a(\mathrm{mod}\,p)$, где p является простым числом, a – квадратичным вычетом по модулю p:

1) выбрать n такое, что $\left(\frac{n}{p}\right)=-1$;

2) найти целые числа e, q, удовлетворяющие соотношению $p-1=2^e q$, где q – нечетное;

3) положить $y \equiv n^q (\mathrm{mod}\, p)$, $r=e$, $x \equiv a^{\frac{q-1}{2}} (\mathrm{mod}\, p)$;

4) положить $b \equiv ax^2 (\mathrm{mod}\, p)$, $x \equiv ax (\mathrm{mod}\, p)$;

5) выполнить цикл. Пока $b \neq 1 (\mathrm{mod}\, p)$ делать:

а) найти наименьшее m, такое, что $b^{2^m} \equiv 1 (\mathrm{mod}\, p)$;

б) положить $t \equiv y^{2^{r-m-1}} (\mathrm{mod}\, p)$, $y \equiv t^2 (\mathrm{mod}\, p)$, $r=m$;

в) $x \equiv xt (\mathrm{mod}\, p)$, $b \equiv by (\mathrm{mod}\, p)$;

6) найденное значение x будет одним из решений сравнения $x^2 \equiv a (\mathrm{mod}\, p)$. Второе решение находится как $p-x$.

Запишем алгоритм Шенкса для сравнения (1.1):

1) при $n=5$ символ Лежанда $\left(\frac{5}{97}\right) = (-1)^{\frac{5-1}{2}\cdot\frac{97-1}{2}} \left(\frac{97}{5}\right) = \left(\frac{2}{5}\right) = (-1)^{\frac{5^2-1}{8}} = -1$;

2) $p-1=97-1=96=2^5 \cdot 3$, то есть $e=5$, $q=3$;

3) положим $y \equiv 5^3 (\mathrm{mod}\, 97) \equiv 28 (\mathrm{mod}\, 97)$, $r=5$,

$x \equiv 62^{\frac{3-1}{2}} (\mathrm{mod}\, 97) \equiv 62 (\mathrm{mod}\, 97) \equiv -35 (\mathrm{mod}\, 97)$;

4) положим $b \equiv 62 \cdot 62^2 (\mathrm{mod}\, 97) \equiv -35 \cdot (-35)^2 (\mathrm{mod}\, 97) \equiv 96 (\mathrm{mod}\, 97) \equiv -1 (\mathrm{mod}\, 97)$,

$x \equiv 62 \cdot 62 (\mathrm{mod}\, 97) \equiv (-35) \cdot (-35) (\mathrm{mod}\, 97) \equiv 61 (\mathrm{mod}\, 97) \equiv -36 (\mathrm{mod}\, 97)$;

5) выполним цикл. Пока $b \neq 1 (\mathrm{mod}\, 97)$ делаем:

I $b \equiv -1 (\mathrm{mod}\, 97)$;

а) наименьшее m, такое, что $(-1)^{2^m} \equiv 1 (\mathrm{mod}\, 97)$, равно 1;

б) положим $t \equiv 28^{2^{5-1-1}} (\mathrm{mod}\, 97) \equiv 28^8 (\mathrm{mod}\, 97) \equiv 22 (\mathrm{mod}\, 97)$,

$y \equiv 22^2 (\mathrm{mod}\, 97) \equiv 96 (\mathrm{mod}\, 97) \equiv -1 (\mathrm{mod}\, 97)$, $r=1$;

в) $x \equiv -36 \cdot 22 (\mathrm{mod}\, 97) \equiv -36 \cdot 22 (\mathrm{mod}\, 97) \equiv 81 (\mathrm{mod}\, 97)$,

$b \equiv -1 \cdot (-1) (\mathrm{mod}\, 97) \equiv 1 (\mathrm{mod}\, 97)$;

$b \equiv 1 (\mathrm{mod}\, 97)$, поэтому цикл завершен;

6) найденное значение $x \equiv 81 (\mathrm{mod}\, 97)$ будет одним из решений сравнения (1.1). Второе решение находится как $x \equiv (97 - 81) (\mathrm{mod}\, 97) \equiv 16 (\mathrm{mod}\, 97)$.

Ответ: $x \equiv 81 (\mathrm{mod}\, 97)$, $x \equiv 16 (\mathrm{mod}\, 97)$.

Задания лабораторной работы

Для заданий лабораторной работы N – номер варианта, который указывается преподавателем. Значения a, b, n, p, d находятся по следующим правилам:

$$a = \begin{cases} 13(3N + 21), N < 10, \\ 11(2N - 5), N > 10, \end{cases} \quad b = \begin{cases} 29(N + 1), N < 10, \\ 23(N - 5), N > 10, \end{cases}$$

$$n = \begin{cases} 30N + 7, N < 10, \\ 15N - 11, N > 10, \end{cases}$$

$$p = \begin{cases} 937, N \equiv 0 (\mathrm{mod}\, 5), \\ 941, N \equiv 1 (\mathrm{mod}\, 5), \\ 947, N \equiv 2 (\mathrm{mod}\, 5), \\ 953, N \equiv 3 (\mathrm{mod}\, 5), \\ 967, N \equiv 4 (\mathrm{mod}\, 5), \end{cases} \quad d = \begin{cases} 20, N \equiv 0 (\mathrm{mod}\, 5), \\ 18, N \equiv 1 (\mathrm{mod}\, 5), \\ 24, N \equiv 2 (\mathrm{mod}\, 5), \\ 30, N \equiv 3 (\mathrm{mod}\, 5), \\ 44, N \equiv 4 (\mathrm{mod}\, 5), \end{cases} \quad q = \begin{cases} 241, N \equiv 0 (\mathrm{mod}\, 5), \\ 233, N \equiv 1 (\mathrm{mod}\, 5), \\ 193, N \equiv 2 (\mathrm{mod}\, 5), \\ 137, N \equiv 3 (\mathrm{mod}\, 5), \\ 113, N \equiv 4 (\mathrm{mod}\, 5), \end{cases}$$

1. Найти *НОД(a,b)* и коэффициенты его линейного разложения.

2. Найти $a^{-1} (\mathrm{mod}\, p)$.

3. Найти символ Лежандра $\left(\frac{n}{p} \right)$.

4. Решить квадратичное сравнение $x^2 \equiv d (\mathrm{mod}\, q)$.

5. Написать программы, реализующие расширенный алгоритм Евклида, поиск мультипликативного обратного элемента в кольце вычетов, поиск символа Лежандра и алгоритм Шенкса.

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?

3 Эллиптические кривые и алгоритмы на эллиптических кривых

3.1 Лабораторная работа 5. Эллиптические кривые над конечными полями

Цель работы: Реализовать нахождение точек эллиптических кривых над конечными полями.

Порядок выполнения лабораторной работы:

1. Изучить основные сведения об эллиптических кривых.
2. Ознакомиться с примерами решения задач.
3. Выполнить задания лабораторной работы.
4. Подготовиться к защите работы.

Теоретические сведения, необходимые для выполнения работы

1 Алгебраической кривой порядка n над полем F называется множество точек (x, y), $x, y \in P$, удовлетворяющих уравнению $f(x, y) = 0$, где $f(x, y)$ – многочлен степени n с коэффициентами из F. Под степенью многочлена понимается максимальная из степеней его одночленов, а под степенью одночлена понимается сумма степеней входящих в него переменных.

2 Пары (x, y) элементов поля F, удовлетворяющие уравнению кривой, называются её точками.

3 Точка (x_0, y_0) кривой $f(x, y) = 0$ называется неособой, если в ней не равны нулю обе частные производные $\frac{\partial f}{\partial x}$ и $\frac{\partial f}{\partial y}$ многочлена $f(x, y)$. Кривая называется неособой, или гладкой, если все её точки неособые. В любой такой точке (x_0, y_0) к кривой можно провести касательную, уравнение которой имеет следующий вид:

$$(x-x_0)\left.\frac{\partial f}{\partial x}\right|_{\substack{x=x_0\\y=y_0}}+(y-y_0)\left.\frac{\partial f}{\partial y}\right|_{\substack{x=x_0\\y=y_0}}=0. \qquad (2.1)$$

4 Неособая (гладкая) кривая третьего порядка над полем F называется эллиптической кривой над тем же полем, если на ней есть хотя бы одна точка. Если даже таких точек нет, то такие точки могут появиться, если рассмотреть эту кривую над каким-нибудь расширением поля F.

Эллиптическую кривую E над полем F можно определить и как множество пар точек $(x,y)\in F^2$, удовлетворяющих уравнению

$$y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6,\ a_i\in F. \qquad (2.2)$$

5 Через *E(F)* обозначается множество пар точек $(x,y)\in F^2$, удовлетворяющих уравнению (2.2), и бесконечно удаленная точка O. Бесконечно удаленная точка O – точка, расположенная бесконечно далеко в положительном направлении оси ординат и рассматриваемая в качестве третьей точки пересечения эллиптической кривой любой вертикальной линией (любая вертикальная линия пересекает кривую в точках (x_1,y_1), (x_2,y_2), O.

6 Эллиптическая кривая E над полем F, характеристики, не равной 2, может быть задана уравнением в нормальной форме Вейерштрасса:

$$y^2=x^3+a_2x^2+a_4x+a_6,\ a_i\in F. \qquad (2.3)$$

Если характеристика поля не равна 2 и 3, то после упрощения левой части, можно получить уравнение следующего вида:

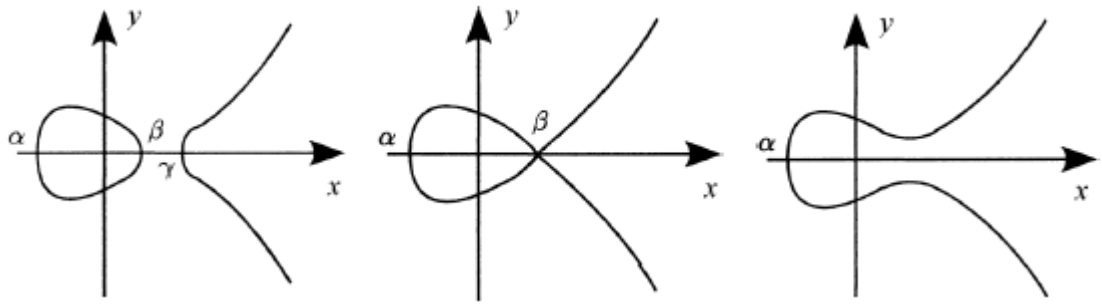
$$y^2=x^3+ax+b,\ \ a,b\in F,\ charF\neq 2,3 \qquad (2.4)$$

7 Для уравнения (2.4) эллиптической кривой E дискриминант имеет следующий вид:

$$\Delta(E) = \left(\frac{a}{3}\right)^3 + \left(\frac{b}{2}\right)^2 = \frac{4a^3 + 27b^2}{4 \cdot 27}. \qquad (2.5)$$

Вид эллиптической кривой в зависимости от значения дискриминанта представлен на рисунке 1.

Кривая E гладкая тогда и только тогда, когда её дискриминант ненулевой.



$\Delta(E) < 0$ $\Delta(E) = 0$ $\Delta(E) > 0$

Рисунок 1 – Вид эллиптической кривой в зависимости от значения дискриминанта

8 Для уравнения (2.4) эллиптической кривой E, не изменяющейся при линейных преобразованиях, j-инвариант имеет следующий вид:

$$j(E) = \frac{1728(4a^3)}{\Delta}. \qquad (2.6)$$

Эллиптические кривые с нулевым j-инвариантом называются суперсингулярными. Если j-инвариант не равен нулю, то эллиптическая кривая называется несуперсингулярной.

9 В криптографических приложениях рассматриваются эллиптические кривые над конечными полями.

Для конечного поля *GF(p)*, где $p > 3$ и p – простое число, уравнение Вейерштрасса имеет следующий вид:

$$y^2 = x^3 + ax + b (\mathrm{mod}\, p), \tag{2.7}$$

где $a, b \in GF(p)$ и $4a^3 + 27b^2 \neq 0 (\mathrm{mod}\, p)$.

Для поля $GF(2^m)$, где $m > 1$ и m – целое число, уравнение Вейерштрасса принимает следующий вид:

$$y^2 + xy = x^3 + ax + b,\ b \neq 0 \tag{2.8}$$

или

$$y^2 + cy = x^3 + ax + b,\ c \neq 0, \tag{2.9}$$

где *a*, *b*, *c* – элементы поля $GF(2^m)$.

Уравнение (2.8) описывает суперсингулярную кривую. Уравнение (2.9) описывает несуперсингулярную кривую.

10 На множестве *E(F)*, состоящем из точек эллиптической кривой и еще одного элемента – бесконечно удаленной точки кривой *O*, можно определить операцию, обладающую свойствами операции абелевой группы. Получающуюся группу рассматривают как аддитивную группу, операцию называют операцией сложения и обозначают знаком плюс. Бесконечно удаленная точка кривой *O* выполняет роль нейтрального элемента (нуля) группы.

По определению для любой точки $(x, y) \in E(F)$

$$(x, y) + O = O + (x, y) = (x, y),\ O + O = O. \tag{2.10}$$

Каждой точке (x, y) эллиптической кривой (2.3) можно поставить в соответствие симметричную точку $(x, \tilde{y}) = (x, -a_1 x - a_3 - y)$. Полагают

$$(x, y) + (x, \tilde{y}) = O. \tag{2.11}$$

Симметричную точку $(x, \tilde{y})$ обозначают $-(x, y)$. На рисунке 2 показана геометрическая интерпретация понятия симметричной точки эллиптической кривой для несуперсингулярных кривых.

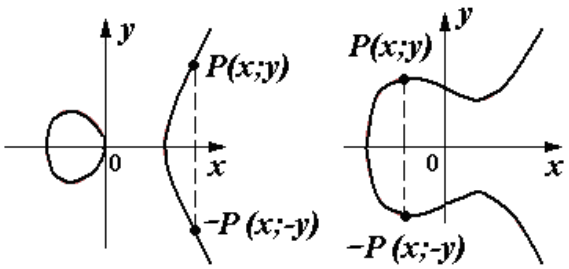


Рисунок 2 – Симметричные точки эллиптических кривых

Суммой двух точек $P(x_1, y_1)$ и $Q(x_2, y_2)$ эллиптической кривой, отличных от O и удовлетворяющих условию $x_1 \neq x_2$, называется точка $R = P + Q$, обратная третьей точке пересечения эллиптической кривой и прямой, проходящей через точки P и Q (рисунок 3).

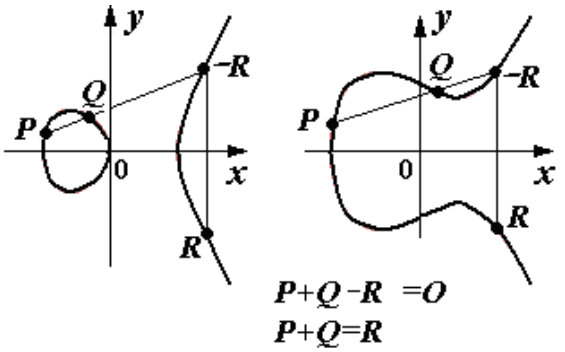


Рисунок 3 – Сложение точек эллиптической кривой

Если суммируемые точки *P* и *Q* совпадают, то *P* + *Q* = *P* + *P* = *R*, что равносильно удвоению точки *2P* = *R*. При *P* = *Q* секущая *PQ* превращается в касательную к кривой и геометрически удвоенная точка *2P* – это точка, обратная к точке пересечения этой касательной и эллиптической кривой (рисунок 4).

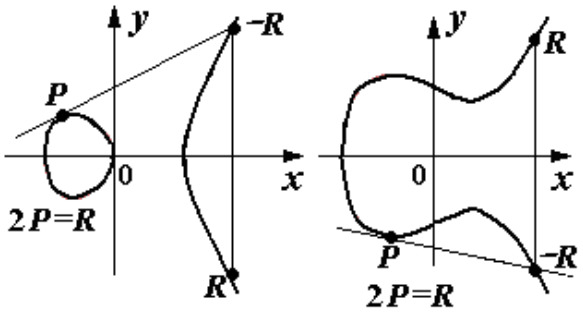


Рисунок 4 – Удвоение точек эллиптической кривой

11 Порядок эллиптической кривой – порядок группы точек эллиптической кривой (число различных точек на эллиптической кривой, включая точку *O*).

12 Поиск всех точек эллиптической кривой над *GF(p)*, где $p > 3$ и *p* – простое число, уравнение Вейерштрасса которой имеет вид $y^2 = x^3 + ax + b(\mathrm{mod}\, p)$, где $a, b \in GF(p)$ и $4a^3 + 27b^2 \neq 0(\mathrm{mod}\, p)$, осуществляется по следующему алгоритму:

– для каждого целого значения *x*, где $0 \le x \le p$, вычислить y^2 по формуле $y^2 = x^3 + ax + b(\mathrm{mod}\, p)$;

– для всех значений y^2 выяснить, будут ли они квадратичными вычетами по модулю *p*. Это можно, например, выяснить, вычислив символ Лежандра $\left(\frac{y^2}{p}\right)$. Если $\left(\frac{y^2}{p}\right) = -1$, то на кривой точек с таким значением *x* нет. Если же корень существует, то найти два значения корня y_1 и y_2. Точки (x, y_1) и (x, y_2) будут принадлежать кривой.

13 Верхняя и нижняя границы для порядка эллиптической кривой определяются теоремой Хассе.

Теорема Хассе. Для порядка N_E группы точек эллиптической кривой над полем GF(q) (q – число элементов поля) справедливо неравенство

$$q+1-2\sqrt{q} \le N_E \le q+1+2\sqrt{q}\,. \qquad (2.12)$$

Примеры решения задач

Задача 1. Найти дискриминант и j-инвариант кривой, заданной уравнением $y^2 = x^3 + 4x + 3$ над полем $GF(5)$. Является ли данная кривая гладкой?

Решение.

Находим дискриминант: $\Delta(E) = \left(4 \cdot 3^{-1}\right)^3 + \left(3 \cdot 2^{-1}\right)^2 (\mathrm{mod}\,5) = 1.$

Находим j-инвариант: $j(E) = \dfrac{1728(4 \cdot 4^3)}{1} (\mathrm{mod}\,5) = 3.$

Так как $\Delta(E) \neq 0$, то кривая является гладкой.

Задача 2. Найти все точки эллиптической кривой, заданной уравнением $y^2 = x^3 + 2x + 4(\mathrm{mod}\,5)$. Чему равен порядок эллиптической кривой?

Решение.

Найдем $x^3 + 2x + 4(\mathrm{mod}\,5)$ и $y^2(\mathrm{mod}\,5)$ для $x, y = \overline{0,4}$. Результаты вычислений оформлены в таблице 11.

Таблица 11 – Результаты поиска значений $x^3 + 2x + 4(\mathrm{mod}\,5)$ и $y^2(\mathrm{mod}\,5)$

x	0	1	2	3	4
$x^3 + 2x + 4(\mathrm{mod}\,5)$	4	2	1	2	1
y	0	1	2	3	4
$y^2(\mathrm{mod}\,5)$	0	1	4	4	1

Группа точек эллиптической кривой состоит из точек (x, y), при которых $x^3 + 2x + 4 (\mathrm{mod} 5)$ и $y^2 (\mathrm{mod} 5)$ равны. Это точки (0,2), (0,3), (2,1), (2,4), (4,1), (4,4) и O.

Порядок эллиптической кривой равен 7.

Задания лабораторной работы

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

$$p = \begin{cases} 17, N \equiv 0 (\mathrm{mod} 5), \\ 19, N \equiv 1 (\mathrm{mod} 5), \\ 23, N \equiv 2 (\mathrm{mod} 5), \\ 29, N \equiv 3 (\mathrm{mod} 5), \\ 31, N \equiv 4 (\mathrm{mod} 5), \end{cases} m = \begin{cases} 5, N \equiv 0 (\mathrm{mod} 3), \\ 4, N \equiv 1 (\mathrm{mod} 3), \\ 3, N \equiv 2 (\mathrm{mod} 3), \end{cases}$$

$$a_i = i + N (\mathrm{mod}\, p),\ i = \overline{1,2},\ b_j = j + N (\mathrm{mod}\, p),\ j = \overline{1,2}.$$

1. Найти дискриминант и j-инвариант кривой, заданной уравнением $y^2 = x^3 + a_1 x + b_1$ над полем $GF(p)$. Определить, является ли данная кривая гладкой.

2. Найти все точки эллиптической кривой, заданной уравнением $y^2 = x^3 + a_2 x + b_2$ над полем $GF(p)$.

3. Найти все точки эллиптической кривой, заданной уравнением $y^2 + xy = x^3 + a_3 x + b_3$ над полем $GF(2^m)$, если $a_3 = g$, $b_3 = g^2$ (g – образующий элемент мультипликативной группы поля $GF(2^m)$).

4. Написать программу, реализующую алгоритмы поиска дискриминанта и j-инварианта кривой, точек эллиптической кривой.

Вопросы для самоконтроля

1 Что называется алгебраической кривой порядка n над полем? Что называется точками кривой?

2 Какая кривая называется прямой? Какая кривая называется кривой второго порядка?

3 Какая точка кривой называется неособой?

4 Какая кривая называется неособой?

5 Что называется касательной кривой?

6 Какая кривая называется эллиптической кривой над полем?

7 Записать форму Вейерштрасса эллиптической кривой.

8 Каким образом осуществляется проективная замена координат?

9 Каким образом записывается уравнение эллиптической кривой в зависимости от характеристики поля?

10 Что называется дискриминантом и j-инвариантом эллиптической кривой?

11 Какие эллиптические кривые называются суперсингулярными? Какие эллиптические кривые называются несуперсингулярными? Каков вид уравнений суперсингулярных и несуперсингулярных кривых?

12 Как вводится операция сложения точек эллиптической кривой?

13 Показать, что множество точек эллиптической кривой с введенной операцией сложения образует абелеву группу.

14 Что называется порядком точки эллиптической кривой?

15 Что называется порядком эллиптической кривой над конечным полем?

16 Сформулировать теорему Хассе.

3.2 Лабораторная работа 6. Алгоритм сложения точек эллиптических кривых

Цель работы: Реализовать алгоритм сложения точек эллиптических кривых над конечными полями.

Порядок выполнения лабораторной работы:

1. Изучить основные сведения, необходимые для выполнения работы.

2. Ознакомиться с примерами решения задач.

3. Выполнить задания лабораторной работы.

4. Подготовиться к защите работы.

Теоретические сведения, необходимые для выполнения работы

1 В соответствии с определением операции сложения в группе точек эллиптической кривой общая схема алгоритма сложения точек $P(x_1, y_1)$ и $Q(x_2, y_2)$ выглядит следующим образом.

Вход: коэффициенты эллиптической кривой, точки *P* и *Q*.

Выход: *R* = *P* + *Q*.

1) Если *P* = *O*, то *R* = *Q*.

2) Если *Q* = *O*, то *R* = *P*.

3) Если *Q* = – *P*, то *R* = *O*.

4) Если $x_1 \neq x_2$, то *R* = *P* + *Q*, иначе *R* = 2*P*.

$R(x_3, y_3)$.

5) Вернуть R.

Координаты x_3, y_3 вычисляются по разным формулам в зависимости от вида эллиптической кривой и условия различия или совпадения точек.

2 Для эллиптических кривых над полем характеристики, большей 3 (то есть для кривых, уравнение которых можно привести к виду $y^2 = x^3 + ax + b$) справедливы следующие утверждения:

– противоположной точкой для точки $P(x,y)$ будет являться $-P(x,-y)$;

– если $P \neq Q$, то формулы для вычисления координат x_3 и y_3 имеют вид $x_3 = \lambda^2 - x_1 - x_2$, $y_3 = \lambda(x_1 - x_3) - y_1$, где $\lambda = \dfrac{y_2 - y_1}{x_2 - x_1}$;

– в случае $P = Q$ формулы имеют вид $x_3 = (\lambda')^2 - 2x_1$, $y_3 = \lambda'(x_1 - x_3) - y_1$, где $\lambda' = \dfrac{3x_1^2 + a}{2y_1}$.

3 Для полей характеристики три (уравнение кривых может быть приведено к виду $y^2 = x^3 + a_2x^2 + a_4x + a_6$) формулы для вычисления координат x_3 и y_3 имеют вид:

– при $P \neq Q$ $x_3 = \lambda^2 - a_2 - x_1 - x_2$, $y_3 = \lambda(x_1 - x_3) - y_1$, где $\lambda = \dfrac{y_2 - y_1}{x_2 - x_1}$;

– при $P = Q$ $x_3 = (\lambda')^2 - a_2 - 2x_1$, $y_3 = \lambda'(x_1 - x_3) - y_1$, где $\lambda' = \dfrac{a_2x_1 - a_4}{y_1}$.

4 Для полей характеристики 2 случаи суперсингулярных и несуперсингулярных кривых рассматриваются отдельно.

Для несуперсингулярных кривых (уравнения которых можно привести к виду $y^2 + xy = x^3 + a_2x^2 + a_6$) точка кривой, противоположная точке $P(x,y)$ имеет координаты $-P(x, x+y)$, а формулы для вычисления координат x_3 и y_3 имеют вид:

– при $P \neq Q$ $x_3 = \lambda^2 + \lambda + a_2 + x_1 + x_2$, $y_3 = x_3 + y_1 + \lambda(x_3 + x_1)$, где $\lambda = \dfrac{y_2 + y_1}{x_2 + x_1}$;

– при $P = Q$ $x_3 = (\lambda')^2 + \lambda' + a_2$, $y_3 = x_1^2 + (\lambda' + 1)x_3$, где $\lambda' = x_1 + \dfrac{y_1}{x_1}$.

Для суперсингулярных кривых (уравнения которых можно привести к виду $y^2 + a_3x = x^3 + a_4x + a_6$) противоположной точкой для $P(x,y)$ будет $-P(x, y + a_3)$, а формулы для вычисления координат x_3 и y_3 имеют вид:

– при $P \neq Q$ $x_3 = \lambda^2 + x_1 + x_2$, $y_3 = a_3 + y_1 + \lambda(x_3 + x_1)$, где $\lambda = \dfrac{y_2 + y_1}{x_2 + x_1}$;

– при $P = Q$ $x_3 = (\lambda')^2$, $y_3 = \lambda'(x_1 + x_3) + y_1 + a_3$, где $\lambda' = \dfrac{x_1^2 + a_4}{a_3}$.

Примеры решения задач

Задача 1. Найти сумму точек $P(2,1)$ и $Q(4,4)$ эллиптической кривой, заданной уравнением $y^2 = x^3 + 2x + 4 (\mathrm{mod}\, 5)$.

Решение.

Кривая задана над полем характеристики, большей 3, и $P \neq Q$, $Q \neq -P$. Тогда для вычисления координат x_3 и y_3 применяются следующие формулы: $x_3 = \lambda^2 - x_1 - x_2$, $y_3 = \lambda(x_1 - x_3) - y_1$, где $\lambda = \dfrac{y_2 - y_1}{x_2 - x_1}$.

По условию $P(2,1)$ и $Q(4,4)$. Тогда $x_1 = 2$, $y_1 = 1$, $x_2 = 4$, $y_2 = 4$.

Находим $\lambda = (4-1)(4-2)^{-1} (\mathrm{mod}\, 5) = 3 \cdot 2^{-1} (\mathrm{mod}\, 5) = 3 \cdot 3 (\mathrm{mod}\, 5) = 4$.

$x_3 = (4^2 - 2 - 4) (\mathrm{mod}\, 5) = 0$, $y_3 = (4 \cdot (2 - 0) - 1) (\mathrm{mod}\, 11) = 2$.

Итак, $P + Q = R$, где $R(0,2)$.

Задача 2. Вычислить $2P$, если $P(3,1)$ – точка эллиптической кривой, заданной уравнением $y^2 = x^3 + 2x + 3 (\mathrm{mod}\, 7)$.

Решение.

Кривая задана над полем характеристики, большей 3, и $P = Q$. Тогда для вычисления координат x_3 и y_3 применяются следующие формулы: $x_3 = (\lambda')^2 - 2x_1$, $y_3 = \lambda'(x_1 - x_3) - y_1$, где $\lambda' = \dfrac{3x_1^2 + a}{2y_1}$.

По условию $P(3,1)$. Тогда $x_1 = 3$, $y_1 = 1$.

Находим $\lambda' = (3 \cdot 3^2 + 2)(2 \cdot 1)^{-1} (\mathrm{mod}\, 7) = 1 \cdot 4 (\mathrm{mod}\, 7) = 4$.

$x_3 = (4^2 - 2 \cdot 3) (\mathrm{mod}\, 7) = 3$, $y_3 = (4(3 - 3) - 1) (\mathrm{mod}\, 7) = 6$.

Итак, $2P = R$, где $R(3,6)$.

Задания лабораторной работы

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

$$p=\begin{cases}17, N\equiv 0(\mathrm{mod}\,5),\\ 19, N\equiv 1(\mathrm{mod}\,5),\\ 23, N\equiv 2(\mathrm{mod}\,5),\\ 29, N\equiv 3(\mathrm{mod}\,5),\\ 31, N\equiv 4(\mathrm{mod}\,5),\end{cases} \quad m=\begin{cases}5, N\equiv 0(\mathrm{mod}\,3),\\ 4, N\equiv 1(\mathrm{mod}\,3),\\ 3, N\equiv 2(\mathrm{mod}\,3),\end{cases}$$

$$a_1=1+N(\mathrm{mod}\,p),\ b_1=1+N(\mathrm{mod}\,p),\ a_2=2+N(\mathrm{mod}\,3),\ b_2=2+N(\mathrm{mod}\,3).$$

1. Найти две точки P и Q эллиптической кривой, заданной уравнением $y^2=x^3+a_1x+b_1$ над полем $GF(p)$. Вычислить $P+Q$ и $2P$.

2. Найти две точки P и Q эллиптической кривой, заданной уравнением $y^2=x^3+a_2x+b_2$ над полем $GF(3)$. Вычислить $P+Q$ и $2P$.

3. Найти две точки P и Q эллиптической кривой, заданной уравнением $y^2+xy=x^3+a_3x+b_3$ над полем $GF(2^m)$, если $a_3=g$, $b_3=g^2$ (g – образующий элемент мультипликативной группы поля $GF(2^m)$). Вычислить $P+Q$ и $2P$.

4. Написать программу, реализующую алгоритм сложения точек эллиптической кривой над конечным полем.

Вопросы для самоконтроля

1 Как вводится операция сложения точек эллиптической кривой?

2 Сформулировать общую схему алгоритма сложения точек эллиптической кривой.

3 Каким образом осуществляется сложение и удвоение точек эллиптических кривых над полями различных характеристик?

4 Сформулировать алгоритм сложения и удвоения для эллиптических кривых над полем характеристики $charF$, $4 \le charF$.

5 Сформулировать алгоритм сложения и удвоения для эллиптических кривых над полем характеристики 3.

6 Сформулировать алгоритм сложения и удвоения для несуперсингулярных эллиптических кривых над полем характеристики 2.

7 Сформулировать алгоритм сложения и удвоения для суперсингулярных эллиптических кривых над полем характеристики 2.

3.3 Лабораторная работа 7. Алгоритм скалярного умножения точек эллиптических кривых

Цель работы: Реализовать алгоритм скалярного умножения точек эллиптических кривых над конечными полями.

Порядок выполнения лабораторной работы:

1. Изучить основные сведения, необходимые для выполнения работы.
2. Ознакомиться с примерами решения задач.
3. Выполнить задания лабораторной работы.
4. Подготовиться к защите работы.

Теоретические сведения, необходимые для выполнения работы

1 Скалярное умножение определяется для каждой точки эллиптической кривой над конечным полем. Если k – целое положительное, то

$$kP = \underbrace{P + P + ... + P}_{k\ раз},$$

где операция + есть операция сложения точек эллиптической кривой.

2 Алгоритм скалярного умножения точек.

Вход: эллиптическая кривая *E*, положительное целое число *k*, точка *P* кривой *E*.

Выход: *kP*.

Алгоритм:

1) Найти двоичное представление числа *k*: $k = k_{n-1} \cdot 2^{n-1} + ... + k_1 \cdot 2^1 + k_0 \cdot 2^0$.

2) Присвоить $R = O$ (бесконечно удаленная точка).

3) Для i от 0 до $n-1$ выполнить следующие действия:

– если $k_i = 1$, то $R = R + P$;

– $P = 2P$.

4) Вернуть: *R*.

Примеры решения задач

Задача 1. Вычислить $5P$, если $P(3,1)$ – точка эллиптической кривой, заданной уравнением $y^2 = x^3 + 2x + 3 (\mathrm{mod}\, 7)$.

Решение.

1) Двоичное представление числа $k = 5 = 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0$, то есть $(k_2, k_1, k_0) = (1,0,1)$

2) $R = O$.

3) $i = 0$;

– $k_0 = 1$; находим $R = R + P = O + P = P$;

– находим $P = 2P$, $P(3,6)$.

$i = 1$;

– $k_1 = 0 \neq 1$;

– находим $P = 2P$, $P(3,1)$.

$i = 2$;

– $k_2 = 1$; находим $R = P + P = 2P$, $R(3,6)$;

– находим $P = 2P$, $P(3,6)$.

4) $5P = R$, $R(3,6)$.

Задания лабораторной работы

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

$$p = \begin{cases} 17, N \equiv 0 (\mathrm{mod}\, 5), \\ 19, N \equiv 1 (\mathrm{mod}\, 5), \\ 23, N \equiv 2 (\mathrm{mod}\, 5), \\ 29, N \equiv 3 (\mathrm{mod}\, 5), \\ 31, N \equiv 4 (\mathrm{mod}\, 5), \end{cases} \quad m = \begin{cases} 5, N \equiv 0 (\mathrm{mod}\, 3), \\ 4, N \equiv 1 (\mathrm{mod}\, 3), \\ 3, N \equiv 2 (\mathrm{mod}\, 3), \end{cases}$$

$a_1 = 1 + N (\mathrm{mod}\, p)$, $b_1 = 1 + N (\mathrm{mod}\, p)$, $a_2 = 2 + N (\mathrm{mod} 3)$, $b_2 = 2 + N (\mathrm{mod} 3)$.

1. Найти точку P эллиптической кривой, заданной уравнением $y^2 = x^3 + a_1 x + b_1$ над полем $GF(p)$. Вычислить kP.

2. Найти две точку P эллиптической кривой, заданной уравнением $y^2 + xy = x^3 + a_3 x + b_3$ над полем $GF(2^m)$, если $a_3 = g$, $b_3 = g^2$ (g – образующий элемент мультипликативной группы поля $GF(2^m)$). Вычислить kP.

3. Написать программу, реализующую алгоритм скалярного умножения точек эллиптической кривой над конечным полем.

Вопросы для самоконтроля

1 Как вводится операция скалярного умножения точек эллиптической кривой?

2 Сформулировать общую схему алгоритма скалярного умножения точек эллиптической кривой.

3.4 Лабораторная работа 8. Алгоритм определения порядка точки на эллиптической кривой

Цель работы: Реализовать алгоритм определения порядка точки на эллиптической кривой.

Порядок выполнения лабораторной работы:

1. Изучить основные сведения, необходимые для выполнения работы.

2. Ознакомиться с примерами решения задач.

3. Выполнить задания лабораторной работы.

4. Подготовиться к защите работы.

Теоретические сведения, необходимые для выполнения работы

1 Чтобы найти порядок n точки P эллиптической кривой $y^2 = x^3 + ax + b$ над полем $GF(p)$, надо решить уравнение $nP = O$.

2 Алгоритм вычисления порядка точки эллиптической кривой.

Вход: эллиптическая кривая *E*, точка *P* кривой *E*.

Выход: n – порядок точки *P*.

1) Вычислить $m = \left\lceil \sqrt{N_1} \right\rceil$ (округление с избытком), где $N_1 = p + 1 + 2\sqrt{p}$ – максимальная оценка порядка группы точек эллиптической кривой, полученная из теоремы Хассе.

2) Построить таблицу пар (t, tP) для $t = 1, 2, ..., m$.

3) Вычислить $Q = -mP$.

4) Положить $R = O$ (бесконечно удаленная точка).

5) Для i от 0 до $m - 1$ выполнить следующие действия:

– проверить, будет ли точка R содержаться в таблице, построенной на шаге 1;

– если найдется *t* такое, что $R = tP$, то считать $n = mi + t$; выход из цикла;

– положить $R = R + Q$.

6) Вернуть *n*.

Примеры решения задач

Задача 1. Найти порядок точки $P(2,4)$ эллиптической кривой, заданной уравнением $y^2 = x^3 + 2x + 4 (\mathrm{mod}\, 5)$.

Решение.

1) Вычисляем $m = \left\lceil \sqrt{N_1} \right\rceil$, где $N_1 = 5 + 1 + 2\sqrt{5} \approx 10,47$. $m = \left\lceil \sqrt{N_1} \right\rceil = 4$.

2) Строим таблицу пар (t, tP) для $t = 1,2,...,m$ (таблица 12).

Таблица 12 – Значения пар (t, tP)

t	1	2	3	4
tP	(2,4)	(0,2)	(4,4)	(4,1)

3) Вычисляем $Q = -mP = -4P$, $Q(4,4)$.

4) Положим $R = O$.

5) $i = 0$;

– точка R не содержится в таблице 12;

– такого t, что $R = tP$, нет;

– положим $R = R + Q$, $R(4,4)$.

$i = 1$;

– точка R содержится в таблице 12;

– при $t = 3$ $R = tP$, тогда считать $n = 4 \cdot 1 + 3 = 7$;

6) $n = 7$.

Итак, порядок точки $P(2,4)$ эллиптической кривой, заданной уравнением $y^2 = x^3 + 2x + 4 (\mathrm{mod}\, 5)$, равен 7.

Задания лабораторной работы

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

$$p = \begin{cases} 17, N \equiv 0 (\mathrm{mod}\, 5), \\ 19, N \equiv 1 (\mathrm{mod}\, 5), \\ 23, N \equiv 2 (\mathrm{mod}\, 5), \\ 29, N \equiv 3 (\mathrm{mod}\, 5), \\ 31, N \equiv 4 (\mathrm{mod}\, 5), \end{cases}$$

$$a = 1 + N (\mathrm{mod}\, p),\ b = 1 + N (\mathrm{mod}\, p).$$

1. Найти точки P и Q эллиптической кривой, заданной уравнением $y^2 = x^3 + ax + b$ над полем $GF(p)$. Определить порядок точек P и Q.

2. Написать программу, реализующую алгоритм поиска порядка точки эллиптической кривой над конечным полем.

Вопросы для самоконтроля

1 Что называется порядком точки эллиптической кривой?

2 Какое уравнение необходимо решить для того, чтобы найти порядок точки эллиптической кривой, заданной уравнением $y^2 = x^3 + ax + b$ над полем $GF(p)$?

3 Сформулировать общую схему алгоритма нахождения порядка точки эллиптической кривой, заданной уравнением $y^2 = x^3 + ax + b$ над полем $GF(p)$.

4 Криптографические приложения эллиптических кривых

4.1 Лабораторная работа 9. Криптографически надежные параметры эллиптических кривых

Цель работы: Реализовать алгоритмы генерации эллиптических кривых над конечными полями и поиска базовой точки кривой.

Порядок выполнения лабораторной работы:

1. Изучить основные сведения, необходимые для выполнения работы.
2. Ознакомиться с примерами решения задач.
3. Выполнить задания лабораторной работы.
4. Подготовиться к защите работы.

Теоретические сведения, необходимые для выполнения работы

1 В настоящее время для целей криптографии обычно используются эллиптические кривые над простым полем и над полем характеристики 2. Для использования эллиптической криптографии участники протокола должны согласовать все параметры, определяющие эллиптическую кривую.

2 При использовании эллиптической кривой в криптографических целях следует определить совокупность параметров, общих для всех участников протокола.

Для эллиптических кривых E над полем $GF(p)$ эти параметры включают:

– простое число p, по модулю которого производятся вычисления;

– коэффициенты $a, b \in GF(p)$ уравнения эллиптической кривой E;

– целое число m – порядок группы точек эллиптической кривой E;

– простое число q – порядок циклической подгруппы группы точек эллиптической кривой E, причем $m = kq$, где k – некоторое положительное целое число;

– базовая точка $P \neq O$ эллиптической кривой E с координатами (x_P, y_P), удовлетворяющая условию $qP = O$.

Для кривых E над полем $GF(2^n)$ эти параметры включают:

– порядок поля n;

– неприводимый многочлен $f(x)$ степени n;

– коэффициенты $a, b \in GF(2^n)$ уравнения эллиптической кривой E;

– целое число m – порядок группы точек эллиптической кривой E;

– простое число q – порядок циклической подгруппы группы точек эллиптической кривой E, причем $m = kq$, где k – некоторое положительное целое число;

– базовая точка $P \neq O$ эллиптической кривой E с координатами (x_P, y_P), удовлетворяющая условию $qP = O$.

Правильный выбор этих величин – нетривиальная задача. Как правило, описание того или иного криптографического протокола включает либо алгоритм формирования параметров кривых, либо фиксированную совокупность допустимых эллиптических кривых и базовых точек.

3 Генерация эллиптической кривой, применяемой в криптографических целях, состоит из следующих шагов:

– генерация характеристики поля Галуа;

– генерация коэффициентов кривой;

– вычисление порядка N_E группы точек кривой;

– генерация базовой точки;

– определение порядка базовой точки кривой (желательно, чтобы $N_E / n \leq 4$).

Примеры решения задач

Задача 1. Описать алгоритм выбора эллиптической кривой над простым конечным полем и базовой точки на ней на основе случайного выбора.

Решение.

1) Выбрать конечное поле *GF(p)*, где $p > 3$ – простое число.

2) Выбрать произвольно тройку чисел $x, y, a \in GF(p)$.

3) Вычислить $b = (y^2 - (x^3 + ax))(\mathrm{mod}\, p)$.

4) Если выполняется условие $4a^3 + 27b^2 \neq 0(\mathrm{mod}\, p)$, то кривая найдена и задается уравнением $y^2 = x^3 + ax + b$ над полем $GF(p)$. В противном случае перейти к шагу 2.

Задания лабораторной работы

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

$$p = \begin{cases} 17, N \equiv 0(\mathrm{mod}\,5), \\ 19, N \equiv 1(\mathrm{mod}\,5), \\ 23, N \equiv 2(\mathrm{mod}\,5), \\ 29, N \equiv 3(\mathrm{mod}\,5), \\ 31, N \equiv 4(\mathrm{mod}\,5), \end{cases} \quad m = \begin{cases} 3, N \equiv 0(\mathrm{mod}\,5), \\ 4, N \equiv 1(\mathrm{mod}\,5), \\ 7, N \equiv 2(\mathrm{mod}\,5), \\ 2, N \equiv 3(\mathrm{mod}\,5), \\ 2, N \equiv 4(\mathrm{mod}\,5). \end{cases}$$

1. Написать программу, реализующую генерацию эллиптической кривой над полем $GF(p)$ и базовую точку на ней.

2. Написать программу, реализующую генерацию эллиптической кривой над полем $GF(2^m)$ и базовую точку на ней.

Вопросы для самоконтроля

1 Какие требования предъявляются к эллиптическим кривым, используемым в криптографических конструкциях?

2 Какая точка называется базовой точкой эллиптической кривой?

3 Перечислить этапы генерации эллиптической кривой.

4 Каким образом осуществляется случайная генерация эллиптической кривой над конечным полем и базовой точки на ней?

4.2 Лабораторная работа 10. Генерация псевдослучайных последовательностей

Цель работы: Реализовать алгоритм генерации псевдослучайных последовательностей.

Порядок выполнения лабораторной работы:

1. Изучить основные сведения, необходимые для выполнения работы.
2. Ознакомиться с примерами решения задач.
3. Выполнить задания лабораторной работы.
4. Подготовиться к защите работы.

Теоретические сведения, необходимые для выполнения работы

1 Генерация псевдослучайных последовательностей является одной из актуальных задач криптографии. Псевдослучайные последовательности используются для секретных ключей в системах симметричного шифрования, генерации паролей, PIN-кодов для различных типов пластиковых карт, кодов аутентификации, вероятностных алгоритмов и систем квантового распределения ключей.

Эллиптические кривые могут использоваться для получения псевдослучайных последовательностей на основе уже известных алгоритмов генерации последовательностей.

2 Алгоритм генерации псевдослучайных последовательностей над эллиптической кривой на основе конгруэнтного генератора следующий:

1) Выбрать конечное поле $GF(q)$.

2) Выбрать кривую E.

3) Выбрать генератор. Например, линейный конгруэнтный генератор, заданный уравнением $X_{i+1} = cX_i + P$.

4) Выбрать фиксированное целое число *c*, начальную точку X_0 и фиксированную точку *P*, причем $cX_0 + P \neq X_0$.

5) Вычислить последовательность состояний генератора X_0, X_1, X_2, …, используя формулу $X_{i+1} = cX_i + P$.

6) Сформировать выходную двоичную псевдослучайную последовательность из младших бит ординат точек X_i, $i = 0,1,2,\ldots$.

3 Алгоритм формирования псевдослучайной последовательности над эллиптической кривой на основе регистров сдвига с линейными обратными связями:

1) Выбираем конечное поле *GF(q)*.

2) Выбираем эллиптическую кривую *E*.

3) Выбираем точку *P* порядка *r* на кривой *E*.

4) Выбираем примитивный многочлен *f(x)* над *GF(q)*. Строим регистр сдвига с линейными обратными связями, используя *f(x)* в качестве характеристического многочлена.

5) Вычисляем последовательность $P_0, P_1, P_2, \ldots$ с использованием *M*-последовательности регистра сдвига.

Примеры решения задач

Задача 1. Найти первые три члена последовательности над эллиптической кривой с уравнением $y^2 = x^3 + 3x + 7 (\mathrm{mod} 11)$ на основе конгруэнтного генератора, заданного уравнением $X_{i+1} = 2X_i + P$, где $P(10,5)$.

Решение.

Выберем начальную точку $X_0(9,2)$.

Найдем $2X_0 + P = 2(9,2) + (10,5) = (5,2) + (10,5) = (10,6) \neq P$.

$X_1 = 2X_0 + P = (10,6)$.

$X_2 = 2X_1 + P = 2(10,6) + (10,5) = (5,2) + (10,5) = (10,6)$.

Задача 2. Найти несколько первых членов последовательности над эллиптической кривой с уравнением $y^2 = x^3 + x + 1 (\mathrm{mod}\, 7)$ на основе инверсивного генератора, заданного уравнением $X_{i+1} = 3X_i^{-1} + P$, где $P(0,6)$. Указать период найденной последовательности. Составить соответствующую двоичную последовательность.

Решение.

Выберем начальную точку $X_0(2,5)$.

$X_1 = 3X_0^{-1} + P = 3(2,5)^{-1} + (0,6) = 3(2,2) + (0,6) = (0,6) + (0,6) = (2,2)$,

$X_2 = 3X_1^{-1} + P = 3(2,2)^{-1} + (0,6) = 3(2,5) + (0,6) = (0,1) + (0,6) = O$,

$X_3 = 3X_2^{-1} + P = 3O + (0,6) = (0,6)$,

$X_4 = 3X_3^{-1} + P = 3(0,6)^{-1} + (0,6) = 3(0,1) + (0,6) = (2,2) + (0,6) = (2,5)$

$X_5 = 3X_4^{-1} + P = 3(2,5)^{-1} + (0,6) = 3(2,2) + (0,6) = (0,6) + (0,6) = (2,2)$.

Период последовательности равен 4.

Найдем двоичную последовательность.

Ордината точки $X_0(2,5)$ равна 5. Переведем 5 в двоичную систему счисления: $5_{10} = 101_2$. Младший бит равен 1 и $u_0 = 1$. Аналогично находим $u_1 = 0$, $u_2 = 0$, $u_3 = 0$, $u_4 = 1, \ldots$. Двоичная последовательность также имеет период 4.

Задания лабораторной работы

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

$$p = \begin{cases} 17, N \equiv 0 (\mathrm{mod}\, 5), \\ 19, N \equiv 1 (\mathrm{mod}\, 5), \\ 23, N \equiv 2 (\mathrm{mod}\, 5), \\ 29, N \equiv 3 (\mathrm{mod}\, 5), \\ 31, N \equiv 4 (\mathrm{mod}\, 5), \end{cases}$$

$$a = 1 + N (\mathrm{mod}\, p),\ b = 1 + N (\mathrm{mod}\, p).$$

1. Найти псевдослучайную последовательность над эллиптической кривой, заданной уравнением $y^2 = x^3 + ax + b$ над полем $GF(p)$ на основе:

а) линейного конгруэнтного генератора;

б) инверсивного генератора;

в) регистра сдвига.

Характеристики генераторов и регистра сдвига подобрать самостоятельно.

2. Написать программу, реализующую генерацию псевдослучайных последовательностей над эллиптической кривой на основе линейного конгруэнтного генератора.

3. Написать программу, реализующую генерацию псевдослучайных последовательностей над эллиптической кривой на основе инверсивного генератора.

4. Написать программу, реализующую генерацию псевдослучайных последовательностей над эллиптической кривой на основе регистров сдвига с линейными обратными связями.

Вопросы для самоконтроля

1 Где применяются псевдослучайные последовательности?

2 Каким образом используются эллиптические кривые для генерации псевдослучайных последовательностей?

3 Сформулировать алгоритм генерации псевдослучайных последовательностей над эллиптической кривой на основе конгруэнтных генераторов.

4 Какие операции над точками эллиптической кривой осуществляются при реализации алгоритма генерации псевдослучайных последовательностей над эллиптической кривой на основе линейного конгруэнтного генератора?

5 Какие операции над точками эллиптической кривой осуществляются при реализации алгоритма генерации псевдослучайных последовательностей над эллиптической кривой на основе инверсивного генератора?

6 Сформулировать алгоритм генерации псевдослучайных последовательностей над эллиптической кривой на основе регистров сдвига с линейными обратными связями.

7 Какие операции над точками эллиптической кривой осуществляются при реализации алгоритма генерации псевдослучайных последовательностей над эллиптической кривой на основе регистров сдвига с линейными обратными связями?

4.3 Лабораторная работа 11. Схема симметричного шифрования на эллиптических кривых

Цель работы: Реализовать схему симметричного шифрования на эллиптических кривых.

Порядок выполнения лабораторной работы:

1. Изучить основные сведения, необходимые для выполнения работы.
2. Ознакомиться с примерами решения задач.
3. Выполнить задания лабораторной работы.
4. Подготовиться к защите работы.

Теоретические сведения, необходимые для выполнения работы

1 Схема симметричного шифрования на эллиптических кривых.

Пусть абонент *A* отправляет сообщение абоненту *B*.

Действия отправителя сообщения (абонент *A* шифрует сообщение, предназначенное для абонента *B*):

– *A* преобразует текст сообщения в точки *M* эллиптической кривой;

– *A* выбирает секретный ключ *K*;

– *A* вычисляет шифртекст *C* по формуле *C* = *M* + *K*.

Действия получателя сообщения (абонент *B* расшифровывает шифртекст *C*):

– *B* вычисляет обратный ключ (–*K*);

– *B* восстанавливает точки кривой *M* по формуле *M* = *C* + (–*K*) и преобразует их в исходный текст сообщения.

Примеры решения задач

Задача 1. Найти точку *M*, принадлежащую эллиптической кривой, заданной уравнением $y^2 = x^3 + x + 1$ над полем $GF(19)$. Зашифровать *M* как открытый текст, получив закрытый текст *C*. Показать процедуру восстановления сообщения.

Решение.

Найдем точку, принадлежащую эллиптической кривой, заданной уравнением $y^2 = x^3 + x + 1$ над полем $GF(19)$.

Выберем произвольно $x = 5$. Находим, что $x^3 + x + 1 \equiv 17 (\mathrm{mod} 19)$.

Выясним, имеет ли решения сравнение $y^2 \equiv 17 (\mathrm{mod} 19)$.

Символ Лежандра $\left(\frac{17}{19}\right) = 1$, то есть 17 является квадратичным вычетом по модулю 19. Значит, сравнение $y^2 \equiv 17 (\mathrm{mod} 19)$ имеет решения.

Найдем решения $y^2 \equiv 17 (\mathrm{mod} 19)$, используя свойства квадратичных вычетов. Так как 17 является квадратичным вычетом по модулю 19, то $17^{\frac{19-1}{2}} \equiv 1 (\mathrm{mod} 19)$ или $17^9 \equiv 1 (\mathrm{mod} 19)$. Умножим обе части последнего сравнения на 17, получим

$17^{10} \equiv 17(\text{mod}19)$ или $\left(17^5\right)^2 \equiv 17(\text{mod}19)$. Тогда y можно найти как $y \equiv 17^5(\text{mod}19) \equiv (-2)^5(\text{mod}19) \equiv 6(\text{mod}19)$.

Итак, точка $M(5,6)$ принадлежит эллиптической кривой, заданной уравнением $y^2 = x^3 + x + 1$ над полем $GF(19)$.

Чтобы зашифровать точку $M(5,6)$ выберем секретный ключ K (K также является точкой кривой). Например, $K = (7, 16)$.

Находим шифртекст C:

$C = M + K = (5, 6) + (7, 16) = (13, 11)$.

Покажем процедуру восстановления сообщения.

Находим обратный ключ $-K = (7, 3)$.

Восстановим открытый текст M: $M = C + (-K) = (13, 11) + (7, 3) = (5, 6)$.

Задания лабораторной работы

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

$$p = \begin{cases} 17, N \equiv 0(\text{mod}5), \\ 19, N \equiv 1(\text{mod}5), \\ 23, N \equiv 2(\text{mod}5), \\ 29, N \equiv 3(\text{mod}5), \\ 31, N \equiv 4(\text{mod}5), \end{cases}$$

$$a = 1 + N(\text{mod}\, p),\ b = 1 + N(\text{mod}\, p).$$

1. Для эллиптической кривой $y^2 = x^3 + ax + b$ над полем $GF(p)$ найти точку M, принадлежащую кривой. Зашифровать M как открытый текст, получив закрытый текст C. Показать процедуру восстановления сообщения.

2. Написать программу, реализующую схему симметричного шифрования на эллиптических кривых.

Вопросы для самоконтроля

1 Какие требования предъявляются к эллиптическим кривым, используемым в криптографических конструкциях?

2 Сформулировать схему алгоритма симметричного шифрования на эллиптических кривых.

3 Какие операции над точками эллиптической кривой осуществляются при реализации алгоритма симметричного шифрования на эллиптических кривых?

4 Какие понятия теории чисел используются при реализации алгоритма симметричного шифрования на эллиптических кривых?

4.4 Лабораторная работа 12. Схема асимметричного шифрования на эллиптических кривых

Цель работы: Реализовать схему асимметричного шифрования на эллиптических кривых.

Порядок выполнения лабораторной работы:

1. Изучить основные сведения, необходимые для выполнения работы.
2. Ознакомиться с примерами решения задач.
3. Выполнить задания лабораторной работы.
4. Подготовиться к защите работы.

Теоретические сведения, необходимые для выполнения работы

1 В алгоритмах асимметричного шифрования на эллиптических кривых должны быть определены следующие открытые параметры, общие для всех пользователей:

– конечное поле $GF(p)$;

– эллиптическая кривая $E(GF(p))$;

– порядок n, который является простым числом;

– базовая точка G порядка n.

2 Процедура генерации ключей осуществляется следующим образом. Каждый пользователь системы генерирует пару ключей следующим образом:

– выбирается случайное целое число d, $1 < d < n-1$;

– вычисляется точка $Q = dG$.

Секретным ключом пользователя является число d, открытым ключом – точка Q.

3 Действия отправителя сообщения (абонент A шифрует сообщение M, предназначенное для абонента B):

– A выбирает случайное целое число k, $1 < k < n-1$;

– A вычисляет точку $(x_1, y_1) = kG$;

– A вычисляет точку $(x_2, y_2) = kQ$, используя открытый ключ Q пользователя B;

– A вычисляет $c_1 = M \oplus x_2$.

Шифртекстом является набор $C = (x_1, y_1, c_1)$.

4 Действия получателя сообщения (абонент B расшифровывает шифртекст C):

– B вычисляет точку $(x_2, y_2) = d(x_1, y_1)$, используя свой секретный ключ d;

– B восстанавливает исходное сообщение $M = c_1 \oplus x_2$.

Примеры решения задач

Задача 1. Зашифровать сообщение $M = 11$, используя алгоритм асимметричного шифрования на эллиптических кривых.

Решение.

1) Находим эллиптическую кривую и базовую точку.

Будем искать кривую над полем $GF(29)$;

Выбираем случайным образом $x = 5$, $y = 19$, $a = 7$.

Находим $b \equiv (y^2 - (x^3 + ax)) (\mathrm{mod}\, p) \equiv (19^2 - (5^3 + 7 \cdot 5)) (\mathrm{mod}\, 29) \equiv 27 (\mathrm{mod}\, 29)$.

Проверяем, что $4a^3 + 27b^2 = 4 \cdot 7^3 + 27 \cdot 27^2 \equiv 1 (\mathrm{mod}\, 29) \neq 0 (\mathrm{mod}\, 29)$.

Итак, уравнение эллиптической кривой над полем $GF(29)$ имеет вид $y^2 = x^3 + 7x + 27$.

Базовая точка кривой $G = (5, 19)$ имеет порядок $n = 29$.

2) Найдем ключи.

Выбираем случайное целое число $d = 3$.

Находим точку $Q = dG = 3(5,19) = (19,1)$.

Секретным ключом пользователя является число $d = 3$, открытым ключом – точка $Q = (19, 1)$.

3) Зашифруем сообщение $M = 11$:

– выбираем случайное целое число $k = 5$;

– вычисляем точку $(x_1, y_1) = kG = 5(5,19) = (6,16)$;

– находим точку $(x_2, y_2) = kQ = 5(19,1) = (23,1)$;

– вычисляем $c_1 = M \oplus x_2$. Находим $M = 11_{10} = 1011_2$, $x_2 = 23_{10} = 10111_2$, тогда $M \oplus x_2 = 11100_2 = 28_{10}$. Итак, $c_1 = 28$.

Шифртекстом является набор $C = (6,16,28)$.

Задача 2. Расшифровать сообщение $C = (6,16,28)$, используя алгоритм асимметричного шифрования на эллиптических кривых, если кривая задана уравнением $y^2 = x^3 + 7x + 27$ над полем $GF(29)$, базовая точка кривой $G = (5, 19)$ имеет порядок $n = 29$, а секретный ключ $d = 3$.

Решение.

По условию $C = (6,16,28)$, то есть $x_1 = 6$, $y_1 = 16$ и $c_1 = 28$.

Найдем точку $(x_2, y_2) = d(x_1, y_1) = 3(6,16) = (23,1)$.

Найдем исходное сообщение:

$M = c_1 \oplus x_2 = 28 \oplus 23 = 11100_2 \oplus 10111_2 = 1011_2 = 11.$

Задания лабораторной работы

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

1. Зашифровать сообщение $M = (N + 50)(\mathrm{mod}\, 23)$, используя алгоритм асимметричного шифрования на эллиптических кривых. Показать процедуру восстановления сообщения.

2. Написать программу, реализующую схему асимметричного шифрования на эллиптических кривых.

Вопросы для самоконтроля

1 Какие требования предъявляются к эллиптическим кривым, используемым в криптографических конструкциях?

2 Сформулировать схему алгоритма асимметричного шифрования на эллиптических кривых.

3 Какие операции над точками эллиптической кривой осуществляются при реализации алгоритма асимметричного шифрования на эллиптических кривых?

4 Какие понятия теории чисел используются при реализации алгоритма асимметричного шифрования на эллиптических кривых?

4.5 Лабораторная работа 13. Протоколы цифровой подписи, основанные на эллиптических кривых

Цель работы: Реализовать схему цифровой подписи на эллиптической кривой.

Порядок выполнения лабораторной работы:

1. Изучить основные сведения, необходимые для выполнения работы.
2. Ознакомиться с примерами решения задач.
3. Выполнить задания лабораторной работы.
4. Подготовиться к защите работы.

Теоретические сведения, необходимые для выполнения работы

1 В схеме цифровой подписи на эллиптической кривой должны быть определены следующие открытые параметры, общие для всех пользователей:

– конечное поле $GF(p)$;

– эллиптическая кривая $E(GF(p))$;

– порядок n, который является простым числом;

– базовая точка G порядка n.

2 Процедура генерации ключей осуществляется следующим образом. Каждый пользователь системы генерирует пару ключей следующим образом:

– выбирается случайное целое число d, $1 < d < n - 1$;

– вычисляется точка $Q = dG$.

Секретным ключом пользователя является число d, открытым ключом – точка Q.

3 Формирование подписи (абонент A подписывает сообщение M):

– A вычисляет хеш-образ сообщения $e = h(M)$;

– A выбирает случайное целое число k, $1 < k < n - 1$;

– A вычисляет точку $(x_1, y_1) = kG$;

– A вычисляет $r = (x_1 + e)(\mathrm{mod}\, n)$;

– A вычисляет $s = (k - rd)(\mathrm{mod}\, n)$, используя свой секретный ключ d. В том случае, если $r = 0$ или $s = 0$, выбор k осуществляется заново.

Подписью сообщения является пара (r, s).

4 Проверка подписи (абонент B проверяет подпись (r, s) абонента А на сообщении M):

– B вычисляет точку $(x_1, y_1) = sG + rQ$, используя открытый ключ Q абонента A;

– B вычисляет хеш-образ сообщения $e = h(M)$;

– B вычисляет $r_1 = (x_1 + e)(\mathrm{mod}\, n)$;

Подпись считается верной, если $r_1 = r$.

Примеры решения задач

Задача 1. Подписать сообщение $M = 91$, используя схему цифровой подписи на эллиптической кривой. Вместо хеш-функции применить функцию возведения в степень по простому модулю.

Решение.

1) Находим эллиптическую кривую и базовую точку.

Будем искать кривую над полем $GF(37)$;

Выбираем случайным образом $x = 9$, $y = 25$, $a = 17$.

Находим $b \equiv (y^2 - (x^3 + ax))(\mathrm{mod}\, p) \equiv (25^2 - (9^3 + 17 \cdot 9))(\mathrm{mod}\, 37) \equiv 2(\mathrm{mod}\, 37)$.

Проверяем, что $4a^3 + 27b^2 = 4 \cdot 17^3 + 27 \cdot 2^2 \equiv 2(\mathrm{mod}\, 37) \neq 0(\mathrm{mod}\, 37)$.

Итак, уравнение эллиптической кривой над полем $GF(37)$ имеет вид $y^2 = x^3 + 17x + 2$.

Базовая точка кривой $G = (9, 25)$ имеет порядок $n = 37$.

2) Найдем ключи.

Выбираем случайное целое число $d = 4$.

Находим точку $Q = dG = 4(9,25) = (9,12)$.

Секретным ключом пользователя является число d = 4, открытым ключом – точка Q = (9, 12).

3) Подпишем сообщение $M = 91$.

Вычисляем $e = h(M)$, применяя функцию возведения в степень по простому модулю. Например, $e = 91^{15} (\mathrm{mod}\, 37) = 14$.

Выбираем случайное целое число k = 2.

Находим точку $(x_1, y_1) = 2G = 2(9,12) = (12,11)$;

Находим $r = (x_1 + e)(\mathrm{mod}\, n) = (12 + 14)(mod\, 37) = 28$;

Находим $s = (k - rd)(\mathrm{mod}\, n) = (2 - 28 \cdot 4)(\mathrm{mod}\, 37) = 1$.

Подписью сообщения $M = 91$ является пара (28, 1).

Задача 2. Проверить подпись (28,1) сообщения $M = 91$ на эллиптической кривой, уравнение которой $y^2 = x^3 + 17x + 2$ над полем $GF(37)$. В качестве базовой точки взять точку G = (9, 25). Открытым ключом является точка Q = (9, 12). Вместо хеш-функции применить функцию $h(t) = t^{15} (\mathrm{mod}\, 37)$.

Решение.

Найдем точку $(x_1, y_1) = sG + rQ = 1(9,25) + 28(9,12) = (9,25) + (12,26) = (12,11)$.

Найдем $e = h(M)$: $e = 91^{15} (\mathrm{mod}\, 37) = 14$.

Найдем $r_1 = (x_1 + e)(\mathrm{mod}\, n) = (12 + 14)(\mathrm{mod}\, 37) = 28$;

Так как $r_1 = r$, то подпись подлинна.

Задания лабораторной работы

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

1. Показать процедуру подписи сообщение $M = (N + 50)(\mathrm{mod}\, 23)$, используя схему цифровой подписи на эллиптической кривой. Вместо хеш-функции

применить функцию возведения в степень по простому модулю. Показать процедуру проверки подписи.

2. Написать программу, реализующую схему цифровой подписи на эллиптической кривой.

Вопросы для самоконтроля

1 Какие требования предъявляются к эллиптическим кривым, используемым в схемах цифровой подписи?

2 Сформулировать схему алгоритма цифровой подписи на эллиптической кривой.

3 Какие операции над точками эллиптической кривой осуществляются при реализации схемы цифровой подписи на эллиптической кривой?

4 Какие понятия теории чисел используются при реализации схемы цифровой подписи на эллиптической кривой?

4.6 Лабораторная работа 14. Протокол распределения ключей на основе эллиптических кривых

Цель работы: Реализовать протокол распределения ключей на эллиптической кривой.

Порядок выполнения лабораторной работы:

1. Изучить основные сведения, необходимые для выполнения работы.
2. Познакомиться с примерами решения задач.
3. Выполнить задания лабораторной работы.
4. Подготовиться к защите работы.

Теоретические сведения, необходимые для выполнения работы

1 В данной лабораторной работе рассматривается протокол, где абоненты *A* и *B* устанавливают общий секретный ключ. Процедуры задания параметров системы и генерации ключей совпадают с процедурами, описанными в теоретических сведениях пунктов 4.4 и 4.5.

2 Пусть абонент *A* имеет секретный ключ *a* и открытый ключ $Q_a = aG = (x_A, y_A)$, абонент *B* имеет секретный ключ *b* и открытый ключ $Q_b = bG = (x_B, y_B)$.

3 Этапы вычисления общего секретного ключа:

1) действия абонента *A*:

– выбирает случайное целое k_A, $1 < k_A < n-1$;

– вычисляет точку $R_A = k_A G$;

– вычисляет точку $(x_1, y_1) = k_A Q_B$;

– вычисляет точку $s_A = (k_A + a x_A x_1) (\mathrm{mod}\, n)$;

– пересылает R_A абоненту *B*;

2) действия абонента *B*:

– выбирает случайное целое k_B, $1 < k_B < n-1$;

– вычисляет точку $R_B = k_B G$;

– вычисляет точку $(x_2, y_2) = k_B Q_A$;

– вычисляет точку $s_B = (k_B + b x_B x_2) (\mathrm{mod}\, n)$;

– пересылает R_B абоненту *A*;

3) действия абонента *A*:

– вычисляет точку $(x_2, y_2) = a R_B$;

– вычисляет общий секретный ключ $K = s_A (R_B + x_B x_2 Q_B)$;

4) действия абонента *B*:

– вычисляет точку $(x_1, y_1) = b R_A$;

– вычисляет общий секретный ключ $K = s_B (R_A + x_A x_1 Q_A)$.

Примеры решения задач

Задача 1. Найти общий секретный ключ абонентов *A* и *B* для системы, эллиптическая кривая которой имеет уравнение $y^2 = x^3 + 7x + 27$ над полем *GF*(29), базовая точка кривой *G* = (5, 19) имеет порядок *n* = 29.

Решение.

Находим секретный и открытый ключ абонента *A*:

– выбираем случайное целое число $a = 4$, $1 < a < 28$;

– находим точку $Q_A = aG = 4(5,19) = (25,15)$.

Секретным ключом абонента *A* является число *a* = 4, открытым ключом – точка $Q_A = (x_A, y_A) = (25,15)$.

Находим секретный и открытый ключ абонента *B*:

– выбираем случайное целое число $b = 7$, $1 < b < 28$;

– находим точку $Q_B = bG = 7(5,19) = (13,13)$.

Секретным ключом абонента *B* является число *b* = 4, открытым ключом – точка $Q_B = (x_B, y_B) = (13,13)$.

Этапы вычисления общего секретного ключа:

1) действия абонента *A*:

– выбор случайного целого $k_A = 6$, $1 < k_A < 28$;

– поиск точки $R_A = k_A G = 6(5,19) = (27,18)$;

– поиск точки $(x_1, y_1) = k_A Q_B = 4(13,13) = (5,10)$;

– поиск точки $s_A = (k_A + a x_A x_1) (\mathrm{mod}\, n) = (6 + 4 \cdot 25 \cdot 5) (\mathrm{mod}\, 29) = 13$;

– $R_A = (27,18)$ отправляется абоненту *B*;

2) действия абонента *B*:

– выбор случайного целого $k_B = 2$, $1 < k_B < 28$;

– поиск точки $R_B = k_B G = 2(5,19) = (10,16)$;

– поиск точки $(x_2, y_2) = k_B Q_A = 2(25,15) = (17,19)$;

– поиск точки $s_B = (k_B + b x_B x_2) (\mathrm{mod}\, n) = (2 + 7 \cdot 13 \cdot 17) (\mathrm{mod}\, 29) = 12$;

– $R_B = (10,16)$ отправляется абоненту *A*;

3) действия абонента *A*:

– поиск точки $(x_2, y_2) = aR_B = 4(10,16) = (17,19)$;

– поиск общего секретного ключа:

$$K = s_A(R_B + x_B x_2 Q_B) = 13((10,16) + 13 \cdot 17(13,13)) = (16,1);$$

4) действия абонента *B*:

– поиск точки $(x_1, y_1) = bR_A = 7(27,18) = (2,22)$;

– поиск общего секретного ключа:

$$K = s_B(R_A + x_A x_1 Q_A) = 12((27,18) + 25 \cdot 5(25,15)) = (16,1).$$

Задания лабораторной работы

1. Найти общий секретный ключ абонентов *A* и *B* для системы, эллиптическая кривая которой имеет уравнение $y^2 = x^3 + 17x + 2$ над полем *GF*(37), базовая точка кривой *G* = (9, 25) имеет порядок *n* = 37.

2. Написать программу, реализующую протокол распределения ключей на эллиптической кривой.

Вопросы для самоконтроля

1 Какие требования предъявляются к эллиптическим кривым, используемым в протоколах распределения ключей?

2 Сформулировать схему протокола распределения ключей на эллиптической кривой.

3 Какие операции над точками эллиптической кривой осуществляются при реализации протокола распределения ключей на эллиптической кривой?

4 Какие понятия теории чисел используются при реализации протокола распределения ключей на эллиптической кривой?

4.7 Лабораторная работа 15. Схема гибридного шифрования на эллиптических кривых

Цель работы: Реализовать схему гибридного шифрования на эллиптических кривых.

Порядок выполнения лабораторной работы:

1. Изучить основные сведения, необходимые для выполнения работы.
2. Ознакомиться с примерами решения задач.
3. Выполнить задания лабораторной работы.
4. Подготовиться к защите работы.

Теоретические сведения, необходимые для выполнения работы

1 Гибридная (или комбинированная) криптосистема – это система шифрования, совмещающая преимущества криптосистемы с открытым ключом с производительностью симметричных криптосистем. Симметричный ключ используется для шифрования данных, а асимметричный для шифрования самого симметричного ключа.

2 В гибридной схеме шифрования на эллиптической кривой процедуры задания параметров системы и генерации ключей совпадают с процедурами, описанными в теоретических сведениях пунктов 4.4 и 4.5.

3 В схеме используются следующие обозначения:

M – сообщение;

Q – открытый ключ абонента B;

d – секретный ключ абонента B;

K_S – сеансовый ключ;

C_M – шифртекст;

C_K – зашифрованный ключ;

E_S – преобразование, описывающее шифрование сообщения с использованием симметричного криптоалгоритма;

D_S – преобразование, описывающее расшифрование сообщения с использованием симметричного криптоалгоритма;

E_A – преобразование, описывающее шифрование сообщения с использованием асимметричного криптоалгоритма;

D_A – преобразование, описывающее расшифрование сообщения с использованием асимметричного криптоалгоритма;

3 Действия отправителя сообщения (абонент *A* шифрует сообщение *M,* предназначенное для абонента *B*):

– *A* вычисляет C_M, преобразуя сообщение *M* на сеансовом ключе K_S с использованием E_S;

– *A* вычисляет C_K, преобразуя на открытом ключе *Q* абонента *B* сеансовый ключ K_S с использованием E_A;

– сообщение для абонента *B* включает закрытый текст C_M и преобразованный ключ C_K.

4 Действия получателя сообщения (абонент *B* расшифровывает полученное сообщение, включающее закрытый текст C_M и преобразованный ключ C_K):

– *B* восстанавливает сеансовый ключ K_S, преобразуя C_K на своем секретном ключе *d* с использованием D_A;

– *B* восстанавливает исходное сообщение *M*, преобразуя C_M на полученном сеансовом ключе K_S с использованием D_S.

Примеры решения задач

Задача 1. Зашифровать сообщение $M = 24$, используя схему гибридного шифрования на эллиптических кривых. Показать процедуру восстановления сообщения.

Решение.

Задаем параметры системы:

– поле $GF(29)$;

– эллиптическая кривая над полем $GF(29)$, уравнение которой имеет вид $y^2 = x^3 + 7x + 27$;

– базовая точка $G = (5, 19)$;

– порядок $n = 29$.

Находим секретный и открытый ключ абонента B:

– выбираем случайное целое число $d = 7$, $1 < d < 28$;

– находим точку $Q = dG = 7(5,19) = (13,13)$.

Секретным ключом абонента B является число $d = 4$, открытым ключом – точка $Q = (13,13)$.

Пусть сеансовый ключ $K_S = (16,1)$.

Покажем, каким образом абонент A шифрует сообщение $M = 24$.

A вычисляет закрытый текст $C_M = M \oplus K_S = 24 \oplus 16 = 8$,

A вычисляет преобразованный ключ C_K:

– выбирает случайное целое число $k = 2$;

– находит точку $(x_1, y_1) = kG = 2(5,19) = (10,16)$;

– находит точку $(x_2, y_2) = kQ = 2(13,13) = (23,28)$;

– вычисляет $C_K = K_s \oplus x_2 = (16,1) \oplus 23 = (7,22)$.

Итак, сообщение, предназначенное для передачи по каналу связи, включает закрытый текст $C_M = 8$, преобразованный ключ $C_K = (7,22)$, а также информацию для получения общего секретного ключа $(x_1, y_1) = (10,16)$.

Рассмотрим процедуру восстановления сообщения. Абонент B расшифровывает полученное сообщение, включающее закрытый текст C_M, преобразованный ключ C_K и (x_1, y_1)

Сначала абонент B восстанавливает общий секретный ключ K_S:

– вычисляет точку $(x_2, y_2) = d(x_1, y_1) = 7(10,16) = (23,28)$;

– находит $K_S = C_k \oplus x_2 = (7,22) \oplus 23 = (16,1)$.

Затем абонент B восстанавливает исходное сообщение:

$$M = C_M \oplus K_S = 8 \oplus 16 = 24.$$

Задания лабораторной работы

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

1. Зашифровать сообщение $M = (N + 50)(\mathrm{mod}\,37)$, используя схему гибридного шифрования на эллиптических кривых. Показать процедуру восстановления сообщения.

2. Написать программу, реализующую схему гибридного шифрования на эллиптических кривых.

Вопросы для самоконтроля

1 Какие требования предъявляются к эллиптическим кривым, используемым в криптографических конструкциях?

2 Сформулировать схему алгоритма гибридного шифрования на эллиптических кривых.

3 Какие операции над точками эллиптической кривой осуществляются при реализации алгоритма гибридного шифрования на эллиптических кривых?

4 Какие понятия теории чисел используются при реализации алгоритма гибридного шифрования на эллиптических кривых?

4.8 Лабораторная работа 16. Российский стандарт на ЭЦП ГОСТ Р 34.10-2012

Цель работы: Изучить основные положения стандарта ЭЦП ГОСТ Р 34.10-2012.

Порядок выполнения лабораторной работы:

1. Изучить основные понятия стандарта ЭЦП ГОСТ Р 34.10-2012.
2. Выполнить задания лабораторной работы.
3. Подготовиться к защите работы.

Теоретические сведения, необходимые для выполнения работы

Теоретическими сведениями является стандарт ЭЦП ГОСТ Р 34.10-2012. Текст стандарта ЭЦП ГОСТ Р 34.10-2012 можно найти на портале Федерального агентства по техническому регулированию и метрологии на странице http://protect.gost.ru/document.aspx?control=7&id=180151.

Задания лабораторной работы

1. Привести свой пример формирования и проверки ЭЦП по алгоритмам, описанным в стандарте ЭЦП ГОСТ Р 34.10-2012.

Вопросы для самоконтроля

1 Над какими полями рассматриваются эллиптические кривые, описываемые в стандарте ЭЦП ГОСТ Р 34.10-2012?

2 Чем обоснована стойкость электронной цифровой подписи стандарта ГОСТ Р 34.10-2012?

3 Какова область применения стандарта ЭЦП ГОСТ Р 34.10-2012?

4 Какие термины и определения используются в стандарте ЭЦП ГОСТ Р 34.10-2012?

5 Какие процессы включает схема (модель) цифровой подписи?

6 Какие математические объекты используются при описании алгоритмов формирования и проверки подписи в стандарте ЭЦП ГОСТ Р 34.10-2012?

7 Каким образом осуществляется формирование цифровой подписи по алгоритму, описанному в стандарте ЭЦП ГОСТ Р 34.10-2012?

8 Каким образом осуществляется проверка цифровой подписи по алгоритму, описанному в стандарте ЭЦП ГОСТ Р 34.10-2012?

Список использованных источников

1 Болотов, А.А. Элементарное введение в эллиптическую криптографию: Алгебраические и алгоритмические основы / А.А. Болотов [и др.]. – Москва: КомКнига, 2006. – 325 с.

2 Иванов, М.А. Криптографические методы защиты информации в компьютерных системах и сетях: учебное пособие / М.А. Иванов, И.В. Чугунков. – Москва: НИЯУ МИФИ, 2012. – 400 с.

3 Пихтильков, С.А. Фундаментальная и компьютерная алгебра: учебное пособие для студентов, обучающихся по программе высшего образования по направлению подготовки 02.03.01 Математика и компьютерные науки / С.А. Пихтильков, О.А. Пихтилькова, Л.Б. Усова. – Оренбург: ОГУ. – 2016. – 116 с.

4 Смарт, Н. Криптография / Н. Смарт. – Москва: Техносфера, 2006. – 528 с.

Приложение А

(справочное)

Символ Лежандра и его свойства

Определение символа Лежандра. Для любого простого нечетного p и целого a символ Лежандра определяется следующим образом:

$$\left(\frac{a}{p}\right)=\begin{cases}0, \ \textit{если} \ \ a\equiv 0(\mathrm{mod}\, p),\\ 1, \ \ \textit{если} \ \ a-\textit{вычет} \ (\mathrm{mod}\, p),\\ -1, \textit{если} \ \ a-\textit{невычет} \ (\mathrm{mod}\, p).\end{cases}$$

Свойства символа Лежандра:

1. $a_1 \equiv a(mod\ p)\Rightarrow\left(\frac{a}{p}\right)=\left(\frac{a_1}{p}\right)$.

2. Критерий Эйлера. $\left(\frac{a}{p}\right)\equiv a^{\frac{p-1}{2}}\ (mod\ p)$.

3. $\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\cdot\left(\frac{b}{p}\right)$.

4. $Если\ \ НОД(a,p)=1\Rightarrow\left(\frac{a^2b}{p}\right)=\left(\frac{b}{p}\right)$.

5. $\left(\frac{1}{p}\right)=1$, $\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$.

6. $\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}=\begin{cases}1, & p\equiv\pm 1(\mathrm{mod}8),\\ -1, & p\equiv\pm 3(\mathrm{mod}8).\end{cases}$

7. Квадратичный закон взаимности. Для любых простых нечетных p и q справедливо $\left(\frac{p}{q}\right)=(-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{q}{p}\right)$.