Министерство науки и высшего образования Российской Федерации

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

Кафедра вычислительной техники и защиты информации

А.А. Рычкова, Е.И. Ряполова

МАТЕМАТИЧЕСКИЕ ОСНОВЫ КРИПТОЛОГИИ

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 10.03.01 Информационная безопасность

Оренбург
2019

УДК 511
ББК 22.131
Р 17

Рецензент – кандидат технических наук Р.Р. Галимов

Рычкова, А.А.
Р 17 Математические основы криптологии: методические указания / А.А. Рычкова, Е.И. Ряполова; Оренбургский гос. ун-т. – Оренбург: ОГУ, 2019. – 56 с.

Основное содержание: алгоритм Евклида, алгоритм Эратосфера; функция Эйлера, подходящие дроби; решение линейных сравнений первой степени; решение системы сравнений первой степени, китайская теорема об остатках; диофантовы уравнения; символ Якоби, символ Лежандра; квадратичные сравнения; полиномы, Поля Галуа.

Методические указания предназначены для выполнения практических работ по дисциплине «Математические основы криптологии» для обучающихся по направлению подготовки 10.03.01 Информационная безопасность.

УДК 511
ББК 22.131

Содержание

Введение

Математические основы криптологии являются базовым курсом для изучения криптографических методов защиты информации, необходимых для подготовки бакалавров, будущая профессиональная деятельность которых связана с обеспечением основных параметров защищенности информации – конфиденциальности и целостности.

Для изучения и понимания сути криптографических методов защиты информации необходимо актуализировать знания и умения математических основ теории чисел и общей алгебры. Основные понятия, теоремы и алгоритмы данных разделов позволят в дальнейшем освоить симметричные и асимметричные криптографические алгоритмы, современные отечественные и зарубежные стандарты шифрования, основные криптографические протоколы.

Методические указания содержат 8практических работ. Каждая работа включает постановку задачи, краткое теоретическое изложение материала, примеры решения практических задач, упражнения к практической работе и контрольные вопросы для самоподготовки.

Методические указания рекомендованы преподавателям как вспомогательный материал в организации и проведении занятий, а также студентам по направлению подготовки 10.03.01 Информационная безопасность, профилю – «Комплексная защита объектов информатизации» – для аудиторного и самостоятельного освоения курса дисциплины «Математические основы криптографии».

1 Практическая работа № 1. Алгоритм Евклида, алгоритм Эратосфена

1.1 Постановка задачи

Цель работы: изучить основные понятия, теоремы и алгоритмы теории чисел, используемые в криптографии.

Задание: научиться решать задачи:

–нахождения наибольшего общего делителя двух чисел на основе алгоритма Евклида;

–нахождения последовательности простых чисел, не превосходящих данного N, на основе алгоритма Эратосфена;

–отыскания функции Эйлера для положительного целого числа.

1.2 Теоретические предпосылки

Основа любого криптографического алгоритма базируется на элементах теории чисел, изучению которых и посвящена данная работа. Теория чисел занимается изучением свойств целых чисел. При изложении теоретического материала мы будем обозначать буквами только целые числа.

Основные понятия

ОпределениеЕсли a делится на b нацело, мы будем говорить, что b делит a. При этом a называется кратным числа b, b – делителем числа a. Число a можно представить как

$$a = q \cdot b, \tag{1.1}$$

где q – полное частное.

Теорема 1Если в равенстве вида $k + l + ... + n = p + q + ... + s$ относительно всех членов, кроме какого-либо одного, известно, что они кратны b, то и этот один член кратен b.

Доказательство:

Пусть таким одним членом будет k. Имеем

$l = b \cdot l_1$

$n = b \cdot n_1$

$p = b \cdot p_1$

$q = b \cdot q_1$

$s = b \cdot s_1$

Перенесем в правую часть равенства все члены, кроме k.

$k = p + q + ... + s - l - ... - n = b \cdot (p_1 + q_1 + ... + s_1 - l_1 - ... - n_1)$

Таким образом, k представляется произведением b на целое число(

$p_1 + q_1 + ... + s_1 - l_1 - ... - n_1$) и тем самым делится на b по определению 1. Что и требовалось доказать.

Теорема 2 (о делении с остатком).

Всякое целое a представляется единственным способом с помощью положительного целого b равенством вида

$$a = b \cdot q + r; \qquad 0 \le r \prec b \tag{1.2}$$

Доказательство

Действительно, одно представление числа a равенством вида (1.2) получим, взяв $b \cdot q$ равным наибольшему кратному числа b, не превосходящему a.

Допустим существование другого представления числа a еще одним равенством вида (1.2)

$$a = b \cdot q_1 + r_1; \qquad 0 \le r_1 \prec b \tag{1.3}$$

Вычтем почленно равенство (1.3) из (1.2), получим

$$0 = b \cdot (q - q_1) + r - r_1 \tag{1.4}$$

Согласно Теореме 1 разность $r - r_1$ кратна b. С другой стороны разность двух неотрицательных чисел меньших b сама будет численно меньше b. Числом кратным b и численно меньшим b является 0. Если $r - r_1 = 0$, то из равенства (1.4) следует, что и $q - q_1 = 0$. Таким образом, второе представление числа a тождественно первому. Теорема 2 доказана.

Число qназывается неполным частным, а число r – остатком от деления a на b.

Наибольший общий делитель

Определение Число, которое делит каждое из чисел a и b, называется общим делителем чисел a и b.

Определение Наибольший из делителей чисел a и b называется наибольшим общим делителем (далее – НОД) этой пары чисел.

Обозначение. НОД (a,b) ≡(a,b).

Определение Если НОД(a,b)=1, то числа a и b называются попарно простыми.

Теорема 3Если a кратно b, то совокупность общих делителей чисел a и b совпадает с совокупностью делителей одного числа b; в частности (a,b)=b.

Доказательство:

Действительно, всякий общий делитель чисел a и b является делителем и одного b. Раз a кратно b, то, согласно Теореме 1, всякий делитель числа b является также делителем числа a, т.е. является общим делителем чисел a и b.

Таким образом, совокупность общих делителей чисел a и b совпадает с совокупностью делителей одного b. Поскольку наибольший делитель числа b есть само b, то (a,b)=b.

Теорема 4Если $a = b \cdot q + r$ (1.3), то совокупность общих делителей чисел a и b совпадает с совокупностью делителей чисел b и c; в частности (a,b)=(b,c).

Доказательство:

Действительно, всякий общий делитель чисел a и b согласно Теореме 3 является и общим делителем чисел b и c. Всякий общий делитель чисел b и c делит a и, следовательно, является общим делителем чисел a и b.

Таким образом, общие делители чисел a и b те же, что и общие делители чисел b и c. В частности, должны совпадать и наибольшие из этих делителей,(a,b)=(b,c).

Алгоритм Евклида. Применяется для отыскания НОД двух чисел.

Пусть a,b – положительные целые и a>b.

Согласно теореме находим ряд равенств:

$$\begin{aligned}
&a = b \cdot q_1 + r_2, && 0 \le r_2 \prec b,\\
&b = r_2 \cdot q_2 + r_3, && 0 \le r_3 \prec r_2,\\
&r_2 = r_3 \cdot q_3 + r_4, && 0 \le r_4 \prec r_{3,}\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&r_{n-2} = r_{n-1} \cdot q_{n-1} + r_n, && 0 \le r_n \prec r_{n-1},\\
&r_{n-1} = r_n \cdot q_n,
\end{aligned} \qquad (1.5)$$

заканчивающийся, когда получается некоторое $r_{n+1}=0$. Последнее неизбежно, так как ряд $b,r_2,r_3,\ldots$ не может содержать более чем b положительных чисел.

Таким образом, НОД чисел аи bравен последнему не равному нулю остатку алгоритма Евклида. Поскольку, согласно Теореме 4

$(a,b) = (b,r_2) = (r_2,r_3) = \ldots = (r_{n-1},r_n) = r_n.$

Простые числа

ОпределениеВсякое a>1 будем называть простым, если у него нет других делителей, кроме 1 и самого себя, иначе – составным.

ОпределениеДва числа называются попарно простыми, если их НОД равен 1.

Алгоритм Эратосфена построения последовательности простых чисел в ряду целых чисел, не превосходящих данного целого N.

Выписываем ряд чисел

$$1,2,\ldots, N \qquad (1.6)$$

Первое простое число в ряду (1.6) – 2. Вычеркиваем из ряда (1.6) все

числа кратные 2, кроме самого числа 2. Первое, оставшееся после 2, простое число – 3. Вычеркиваем из ряда (1.6) все числа кратные 3, кроме самого числа 3. Первое, следующее за 3, невычеркнутое простое число 5. Вычеркиваем из ряда (5) все числа кратные 5, кроме числа 5. И т.д.

Когда указанным способом вычеркнуты все числа, кратные простых, меньше простого p, то все невычеркнутые меньшие p^2 будут простые.

Выводы (без доказательства):

1) приступая к вычеркиванию кратных простогор, это вычеркивание следует начать с p^2;

2) составление последовательности простых чисел, не превосходящих N, закончено, как только вычеркнуты все составные кратные простых, не превосходящих $\sqrt{N}$.

Теорема 5 Всякое целое, большее единицы, разлагается на произведение простых сомножителей и притом единственным способом:

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_K^{\alpha_K}, \qquad (1.7)$$

где $p_1,\ldots,p_K$– простые сомножители числа a,

$\alpha_1,\ldots,\alpha_K$– кратности вхождения соответственно сомножителей $p_1,\ldots,p_K$ в число a.

Разложение (1.7) числа a на простые сомножители называется *каноническим.*

Теорема 6 НОД нескольких чисел является произведением степеней вида p^{α}, где p – общий простой делитель всех этих чисел; α - наименьший из показателей, с которыми p входит в их канонические разложения.

1.4 Примеры решения практических заданий

Пример

Необходимо найти НОД нескольких чисел НОД(50, 160, 1960)

Используя теорему 5, представим каждое число через каноническое разложение:$50=2^1\cdot5^2$ $160=2^5\cdot5^1$ $1960=2^3\cdot5^1\cdot7^2$

Согласно теореме 6:

НОД(50, 160, 1960)$=2^1\cdot5^1=10$

Пример. Отыскать НОД(25,9)

$$25 = 9 \cdot 2 + 7$$
$$9 = 7 \cdot 1 + 2$$
$$7 = 2 \cdot 3 + 1$$
$$2 = 1 \cdot 2 + 0$$
$$НОД(25,9) = 1$$

Пример

Доказать, являются ли числа попарно простыми:

(78, 53)
78 = 53·1+25
53 = 25·2+3
25 = 3·8+1
3 = 1·3 + 0
НОД = 1,
Числа 78 и 53 попарно простые

(189, 115)
189 = 115·1+74
115 = 74·1+41
74 = 41·1 + 33
41 = 33·3+8
33 = 8·4 + 1
8 = 1·8 + 0
НОД = 1
Числа 189 и 115 попарно простые

1.5 Упражнения к практической работе

1 Используя алгоритм Евклида найти наибольший общий делитель двух чисел (k – порядковый номер в списке группы):

НОД(48+k, 2059)
НОД(46188-k, 4709)

2 Найдите НОД(396,1452), НОД(525, 231), НОД(248, 956), НОД(48, 457)

3 Определить, являются ли числа попарно простыми:
(335+k, 231-k)

4 Используя следствие алгоритма Эратосфена доказать, что число простое
1887
573

5Найти НОД нескольких чисел
НОД(81 719, 52003, 33 649, 30107)
НОД(6791400,178500,27720)
НОД(120, 1260, 4950)
НОД(36, 536, 1036)

6Найти каноническое разложение чисел:
2156+2k; 1934-3k

1.6 Контрольные вопросы

1. Докажите теорему о делении с остатком.
2. Дайте понятие НОД двух чисел? Какой алгоритм используется для его нахождения?
3. Какие числа называются простыми, составными?
4. Расскажите алгоритм нахождения последовательности простых чисел.
5. Какое разложение целого числа называется каноническим?

2 Практическая работа № 2. Функция Эйлера. Подходящие дроби

2.1 Постановка задачи

Цель работы: изучить основные понятия, теоремы и алгоритмы теории чисел, используемые в криптографии

Задание: научится решать задачи:
–нахождения функции Эйлера;
–нахождения непрерывной и подходящих дробей.

2.2 Теоретические предпосылки

Определение Функцией Эйлера $\varphi(a)$ называется функция, которая для $\forall a \in Z_+$, равна количеству чисел в ряду от 1 до a-1 попарно простых с a, где $a \geq 1$.

Пример.

$\varphi(1)=1$	$\varphi(4)=2$	$(1,3)$
$\varphi(2)=1$	$\varphi(5)=4$	$(1,2,3,4)$
$\varphi(3)=2$	$\varphi(6)=2$	$(1,5)$

ТеоремаПусть $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ – каноническое разложение числа a. Тогда имеем

$$\varphi(a) = a \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right)$$

или также

$$\varphi(a) = \left(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}\right) \cdot \left(p_2^{\alpha_2} - p_2^{\alpha_2 - 1}\right) \cdot \ldots \cdot \left(p_k^{\alpha_k} - p_k^{\alpha_k - 1}\right).$$

(доказательство рассмотреть самостоятельно).

В частности, если p – простое, то $\varphi(p) = p - 1$.

Непрерывные и подходящие дроби

Непрерывная дробь:

(2.1)

$$\frac{a}{b} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ldots + \cfrac{1}{q_{n-1} + \cfrac{1}{q_n}}}}$$

представляет собой непрерывную дробь для рационального числа.

Числа $q_1,q_2,\ldots$, участвующие в разложении числа α в непрерывную дробь, называются неполными частными (в случае рационального α это будут неполные частные последовательных делений алгоритма Евклида).

Дроби $\delta_1 = q_1, \quad \delta_2 = q_1 + \frac{1}{q_2}, \quad \delta_3 = q_1 + \frac{1}{q_2 + \frac{1}{q_3}}, \quad \ldots$ называются подходящими дробями.

Существуют более удобный способ нахождения подходящих дробей по следующему алгоритму:

1. Ищем неполные частные, реализовав алгоритм Евклида ($q_1,q_2,\ldots,q_n$).
2. Обозначаем $P_0=1$ $Q_0=0$ $P_1=q_1Q_1=1$.
3. Находим

$$P_n = q_n \cdot P_{n-1} + P_{n-2}$$

$$Q_n = q_n \cdot Q_{n-1} + Q_{n-2}$$

4. Рассчитываем подходящие дроби для всех n

$$\delta_n = \frac{P_n}{Q_n}$$

Пример Пусть имеется рациональная дробь $\frac{91}{29}$, необходимо построить непрерывную дробь, найти неполные частные, непрерывную и подходящие дроби.

Решение:

1. Ищем неполные частные по алгоритму Евклида:

$91 = 29 \cdot 3 + 4 \qquad q_1 = 3$

$29 = 4 \cdot 7 + 1 \qquad q_2 = 7$

$4 = 1 \cdot 4 \qquad q_3 = 4$

Непрерывная дробь:

$$\frac{91}{29} = 3 + \frac{1}{7 + \frac{1}{4}}$$

2. Обозначаем $P_0=1$ $Q_0=0$ $P_1=q_1=3Q_1=1$
3. Находим P_nиQ_n, числители и знаменатели для подходящих дробей δ_n:
   $P_1=q_1=3$
   $Q_1=1$

$$P_2 = q_2 \cdot P_{2-1} + P_{2-2} = q_2 \cdot P_1 + P_0 = 7 \cdot 3 + 1 = 22$$

$$Q_2 = q_2 \cdot Q_{2-1} + Q_{2-2} = q_2 \cdot Q_1 + Q_0 = 7 \cdot 1 + 0 = 7$$

$$P_3 = q_3 \cdot P_{3-1} + P_{2-2} = q_3 \cdot P_2 + P_1 = 4 \cdot 22 + 3 = 91$$

$$Q_3 = q_3 \cdot Q_{3-1} + Q_{3-2} = q_3 \cdot Q_2 + Q_1 = 4 \cdot 7 + 1 = 29$$

4. Рассчитываем подходящие дроби:

$$\delta_1 = \frac{P_1}{Q_1} = \frac{3}{1}$$

$$\delta_2 = \frac{P_2}{Q_2} = \frac{22}{7}$$

$$\delta_3 = \frac{P_3}{Q_3} = \frac{91}{29}$$

Ответ: Неполные частные: $\begin{matrix} q_1 = 3 \\ q_2 = 7 \\ q_3 = 4 \end{matrix}$ Непрерывная дробь: $\frac{91}{29} = 3 + \frac{1}{7 + \frac{1}{4}}$

Подходящие дроби: $\delta_1 = \frac{3}{1}, \delta_2 = \frac{22}{7}, \delta_3 = \frac{91}{29}$

2.3 Примеры решения практических заданий

Пример

$\varphi(1)=1$	$\varphi(4)=2$	$(1,3)$
$\varphi(2)=1$	$\varphi(5)=4$	$(1,2,3,4)$
$\varphi(3)=2$	$\varphi(6)=2$	$(1,5)$

Пример

φ(26)=6

26 = 1, 3, 5 , 7 , 9 , 11

Пример

φ(180)=(2^2-2^1)(3^2-3^1)(5^1-5^0)=2·6·4=48

φ(2277)= (3^2-3^1)(11^1-11^0)(23^1-23^0)=1320

φ(3672)=(2^3-2^2)(3^3-3^2)(17^1-17^0)=(4·18·16)=1152

Пример

Найти функцию Эйлера: 1732, 1835, 2378

φ (1732)

1732 = 4· 433

φ (1732) = (4 – 2) · (433 – 1) = 864

φ (1835)

1835 = 5 · 367

φ (1835) = (5-1)·(367-1) = 1464

φ (2378)

$2378 = 2 \cdot 29 \cdot 41$

$\varphi(2378) = (2-1)\cdot(29-1)\cdot(41-1)=1120$

Пример $18 = 2^1 \cdot 3^2$

Пример

$\varphi(1)=1$ $\varphi(4)=2$ $(1,3)$

$\varphi(2)=1$ $\varphi(5)=4$ $(1,2,3,4)$

$\varphi(3)=2$ $\varphi(6)=2$ $(1,5)$ и тт.д

Пример

Представить в виде непрерывной дроби:

113/78

$113 = 78 \cdot 1+35$

$78 = 35 \cdot 2 + 3$

$35 = 3 \cdot 11 + 2$

$3 = 2 \cdot 1 + 1$

$2 = 1 \cdot 2 + 0$

$$\frac{113}{78} = 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{4 + \frac{1}{8}}}}$$

Пример

Представить в виде непрерывной дроби:

152/52

$152 = 52 \cdot 2 + 48$

$52 = 48 \cdot 1+4$

$48=4 \cdot 12+0$

$$\frac{152}{52} = 2 + \frac{1}{1 + \frac{1}{12}}$$

Пример

Представить в виде непрерывной дроби:

47/120

$47 = 120 \cdot 0+47$

$120 = 47 \cdot 2 + 26$

$47 = 26 \cdot 1+21$

$26=21 \cdot 1+5$

$21=5 \cdot 4+1$

$5=1 \cdot 5+0$

$$\frac{47}{120} = \frac{1}{2 + \frac{1}{1 + \frac{1}{1 + \frac{1}{4 + \frac{1}{5}}}}}$$

Пример

Представить в виде непрерывной дроби:

132/148
132 = 148·0+132
148=132·1+16
132=16·8+4
16=4·4+0

$$\frac{132}{148} = \frac{1}{1+\frac{1}{8+\frac{1}{4}}}$$

2.4 Упражнения к практической работе

1Найти функцию Эйлера
а) φ(3672) φ(3519)
б) φ(5040) φ(1683)
в) φ(1409) φ(243)
г) φ(367) φ(573)

2Построить непрерывную дробь и найти неполные частные и подходящие дроби.
а)114/59 , 247/569
б)5391/3976, 125/92
в) 648/35, 125/78
г) 45/263 38/145

3 НайтифункциюЭйлера:
φ(3432)
φ(2277)
φ(3672)
φ(3519)

4Построить непрерывную дробь и найти неполные частные и подходящие дроби
а)112/53 , 217/367
б)51/76, 225/97
в) 448/57, 125/86
г) 45/253, 318/145

5Найти функцию Эйлера
а) φ(372) φ(3619)
б) φ(543) φ(1781)
в) φ(142) φ(2143)
г) φ(357) φ(5173)

2.5 Контрольные вопросы

1 Что показывает функция Эйлера, как она рассчитывается?
2 Дать определение непрерывнойи подходящим дробям.
3 Как рассчитываютсянепрерывная и подходящие дроби?
4 Выведите алгоритм быстрого нахождения подходящих дробей.

3 Практическая работа № 3. Решение линейных сравнений первой степени

3.1 Постановка задачи

Цель работы: изучить основные понятия сравнимых по модулю чисел, расширенный алгоритм Евклида и его применение для нахождения обратного элемента (мультипликативной инверсии) и способы решения линейныхсравнений первой степени.

Задание:

1) Научиться применять РАЕ для нахождения мультипликативной инверсии (обратного элемента);
2) Научится решать линейные сравнения:

– с помощью функции Эйлера;

– с помощью подходящихдробей.

3.2 Теоретические предпосылки

Линейные сравнения с одним неизвестным

ОпределениеПусть m – некоторое целое положительное число m>1. Пусть a и b – это числа, которые при делении на m имеют один и тот же остаток:

$a = m \cdot t_1 + r \qquad 0 \le r < m$

$b = m \cdot t_2 + r$

Числа a и b будем называть **равноостаточными**.

Очевидно, таких чисел бесчисленное множество, т.е. они образуют класс чисел равноостаточных по модулю m или, как говорят, **сравнимых по модулю m**.

Обозначение. $a = b \bmod m$.

Пример. $7 = 10 \bmod 3 \qquad 7 = 10 + 3 \cdot (-1)$.

Все сравнимые числа отличаются на кратное число модулей и поэтому могут быть представлены в виде $a = b + m \cdot t$.

Расширенный алгоритм Евклида (далее РАЕ)

Применяется для вычисления НОД(a,b), b≠0 и получения линейного представления вида НОД(a,b) = ax+by, x,y∈Z.

Вычисляем по формуле следующий ряд:

$a_i = a_{i-2} - a_{i-1}q_{i-1}$,

$x_i = x_{i-2} - x_{i-1}q_{i-1}$,

$y_i = y_{i-2} - y_{i-1}q_{i-1}$,

$q = \frac{a_{i-1}}{a_{i-2}}$, i≥2

Приа$_0$=a, x_0=1, y_0=0, a_1=b, x_1=0, y_1=1, $q = \frac{a_0}{a_1}$, значенияа$_i$, x_i, y_i, до тех пор, пока не получим некотороеа$_{m+1}$=0. Тогда НОД(a,b)=a_m=ax_m+by_m.

Для удобства вычислений применяют следующую таблицу:

i	a_i	x_i	y_i	q_i
0	a	1	0	-
1	b	0	1	$[a_0/a_1]$
2	$a_2=a_0-a_1q_1$	$x_2=x_0-x_1q_1$	$y_2=y_0-y_1q_1$	$[a_1/a_2]$
3	$a_3=a_1-a_2q_2$	$x_3=x_1-x_2q_2$	$y_3=y_1-y_2q_2$	$[a_2/a_3]$
…	…	…	…	…
m+1	0			

Рассмотрим кратко понятия аддитивной и мультипликативной инверсий:

Аддитивная инверсия a+b=0(modn)

Мультипликативная инверсия:

a·b=1(modn)

Пример, 3·7=1(mod 10)

a·a^{-1}=1modn. Мультипликативная инверсия существует, если НОД(n,a)=1.

Пример, 8 mod 10 не имеет мультипликативную инверсию, поскольку НОД(10, 8)=2.

Для нахождения мультипликативной инверсии (или обратного элемента) применяется Расширенный алгоритм Евклида (РАЕ):

ax+by=НОД(a,b)

Пусть a=n:

nx+by=НОД(n,b)

(nx+by=1)modn

nxmodn+bymodn =1modn

bymodn =1modn

y в РАЕ – мультипликативная инверсия.

Найти обратный элемент:

1. 33^{-1} mod 11

a = 11 b = 33 (n; a) = (11; 33) = 11 =>нет обратного элемента

2. 32^{-1} mod 11

32 mod 11 = 1

i	a_i	y_i	q_i
0	11	0	-
1	32	1	0
2	11	0	2
3	10	1	1
4	1	-1	10
5	0		

Y = -1 => 32^{-1}mod 11 = -1

-1 mod 11 = 10
32 · 10 = 1 mod 11
320 mod 11 = 1

Сравнение первой степени, или линейное сравнение

$a \cdot x + b = 0 \bmod m$

можно представить в виде:

$a \cdot x = b \bmod m$

перенесением свободного члена в правую часть.

Среди множества различных линейных сравнений, нас будут интересовать только те, для которых выполняется следующее условие (a,b)=1, поскольку в этом случае линейное сравнение будет иметь решение и притом единственное.

Рассмотрим алгоритм решения линейного сравнения, основанный на алгоритме Евклида.

1. С помощью алгоритма Евклида находят вектор неполных частных $q_1, \ldots, q_n$ для чисел m и a (порядок чисел в данном случае принципиален).

2. Делают обозначение: $P_0=1$, $P_1=q_1$.

3. По формуле

$P_i = q_i \cdot P_{i-1} + P_{i-2}$

находят значения вектора P_i для i=2..n-1.

4. Решение линейного сравнения находят по формуле:

$x = (-1)^{n-1} \cdot P_{n-1} \cdot b \bmod m$

Сравнение 1-ой степени, или линейное сравнение $a \cdot x + b = 0 \bmod m$ можно представить в виде:

$$a \cdot x = b \bmod m$$

перенесением свободного члена в правую часть.

Исследуем вопрос о количестве решений сравнений вида.

1. Для случая $(a,m)=1$ существует **1 решение**.
2. Пусть $(a,m)=d \quad d>1$

$$a = a_1 \cdot d \qquad m = m_1 \cdot d \qquad (a_1, m_1) = 1.$$

2а) d не делит b – **решений нет**.

2б) d делит b. $b = b_1 \cdot d$ – **d - решений**

$a_1 \cdot d \cdot x = (b_1 \cdot d) \bmod (m_1 \cdot d) \Rightarrow$ св-во 6 (над сравнимыми числами)

Для решения необходимо сократить исходное линейное сравнение на di найти одно решение

$a_1 \cdot x = b_1 \bmod m_1$

$(a_1, m_1) = 1 \Rightarrow$ существует единственное решение сравнения по модулю m_1:

$$x = x_1 \bmod m_1 \quad .$$

По модулю m числа образуют столько решений, сколько чисел найдется в ряде 0,1,…,m-1.

Числа $x_1 + 0 \cdot m_1, x_1 + 1 \cdot m_1, x_1 + 2 \cdot m_1, \ldots, x_1 + (d-1) \cdot m_1$ **являются решениями**

сравнения по модулю m.

Вывод: Пусть $(a,m)=d$. Сравнение $a\cdot x=b \bmod m$ невозможно, если b не делится на d. При b, кратном d, сравнение имеет d решений.

Способы решения линейных сравнений (случай $(a,m)=1$).

1. Согласно теореме Эйлера для $(a,m)=1$ и m>1 $a^{\varphi(m)}=1 \bmod m$.

Умножим левую и правую части этого сравнения на целое число b:

$$a^{\varphi(m)}\cdot b=b \bmod m$$

$$a\cdot x=b \bmod m \Rightarrow \quad a\cdot x=\left(a^{\varphi(m)}\cdot b\right)\bmod m$$

$$x=\left(a^{\varphi(m)-1}\cdot b\right)\bmod m$$

$$\boxed{x=\left(a^{\varphi(m)-1}\cdot b\right)\bmod m}$$

2. Рассмотрим способ, основанный на теории подходящих дробей.

Разложим в непрерывную дробь отношение $\frac{m}{a}$:

$$\frac{m}{a}=q_1+\cfrac{1}{q_2+\cfrac{1}{q_3+\ldots}}$$

$$+\frac{1}{q_n}$$

Рассмотрим две последние подходящие дроби: $\frac{P_{n-1}}{Q_{n-1}}, \frac{P_n}{Q_n}=\frac{m}{a}$.

Согласно свойствам непрерывных дробей имеем:

$m\cdot Q_{n-1}-a\cdot P_{n-1}=(-1)^n$.

Вычислим левую и правую часть по модулю m:

$$\left(\underset{=0}{m}\cdot Q_{n-1}\right)\bmod m-\left(a\cdot P_{n-1}\right)\bmod m=(-1)^n \bmod m$$

$$\left(a\cdot P_{n-1}\right)\bmod m=(-1)^{n-1} \bmod m$$

$$\left((-1)^{n-1}\cdot a\cdot P_{n-1}\right)\bmod m=1 \bmod m$$

$$\left((-1)^{n-1}\cdot a\cdot P_{n-1}\cdot b\right)\bmod m=b \bmod m$$

$$a\cdot x=b \bmod m \Rightarrow$$

$$x=\left((-1)^{n-1}\cdot P_{n-1}\cdot b\right)\bmod m.$$

$$\boxed{x=\left((-1)^{n-1}\cdot P_{n-1}\cdot b\right)\bmod m.}$$

Первообразные корни

Пусть $(a,m)=1$, тогда на основании т. Эйлера

$$a^{\varphi(m)}=1 \bmod m$$

$\exists$ ли другие показатели γ, для которых:

$$a^{\gamma}=1 \bmod m.$$

Нас будут интересовать такие $\gamma : \gamma \le \varphi(m)$.

Наименьшее из чисел $\gamma : \delta = \min \gamma : a^{\gamma} = 1 \bmod m$ будем называть показателем, которому $a \in$ по $\bmod m$. Если $\delta = \varphi(m)$, то число а называется первообразным корнем по $\bmod m$.

3.3 Примеры решения практических заданий

Пример

Рассмотрим второй способ решения (через подходящие дроби)

$x = \left((-1)^{n-1} \cdot P_{n-1} \cdot b\right) \bmod m.$

Находим неполные частные

$3=8\cdot 0+3$ $q_1=0$

$8=3\cdot 2+2$ $q_2=2$

$3=2\cdot 1+1$ $q_3=1$

$2=1\cdot 2+0$ $q_4=2$

n=4 (по количеству неполных частных)

Таким образом, для решения линейного сравнения нам необходимо найти P_3

$P_0=1$ $P_1=q_1=2$

$P_n=q_n\cdot P_{n-1}+P_{n-2}$

$P_2=q_2\cdot P_1+P_0=2\cdot 2+1=5$

$P_3=q_3\cdot P_2+P_1=1\cdot 5+2=7$

$$x = \left((-1)^{n-1} \cdot P_{n-1} \cdot b\right) \bmod m. = ((-1)^3 \cdot 7 \cdot 2) \bmod 3 = -14 \bmod 3 = 1 \bmod 3$$

Пример. Решить линейное сравнение $7x = 5 \bmod 19$

Решение

Находим неполные частные с использованием алгоритма Евклида для чисел m и a.

$19 = 7 \cdot 2 + 5$ $q_1 = 2$

$7 = 5 \cdot 1 + 2$ $q_2 = 1$

$5 = 2 \cdot 2 + 1$ $q_3 = 2$

$2 = 1 \cdot 2$ $q_4 = 2$

n=4

$P_0=1$, $P_1=q_1$.

$P_2 = q_2 \cdot P_1 + P_0$ $P_2 = 1 \cdot 2 + 1 = 3$

$P_3 = q_3 \cdot P_2 + P_1$ $P_3 = 2 \cdot 3 + 2 = 8$

$$x = (-1)^3 \cdot P_3 \cdot b \bmod m = (-1) \cdot 8 \cdot 5 \bmod 19 = -40 \bmod 19 = -2 \bmod 19 = 17 \bmod 19$$

Пример

$8 \cdot x = 2 \bmod 3$ $\quad (8,3) = 1 \Rightarrow$ сравнение имеет единственное решение.

Рассмотрим первый способ решения (через функцию Эйлера)

$x = \left(a^{\varphi(m)} \cdot b\right) \bmod m$

$\varphi(3) = 3 - 1 = 2$

$x = \left(8^{(\varphi(3)-1)} \cdot 2\right) \bmod 3 = (8 \cdot 2) \bmod 3 = 16 \bmod 3 = 1 \bmod 3.$

Пример Найти показатель числа 2 по mod 7.

$2^1 = 2 \bmod 7$

$2^2 = 4 \bmod 7 \Rightarrow \delta = 3 \Rightarrow 2$ не является первообразным корнем.

$2^3 = 1 \bmod 7$

Пример Найти показатель числа 3 по mod 7.

$3^1 = 3 \bmod 7$

$3^2 = 2 \bmod 7$

$3^3 = 6 \bmod 7$

$3^4 = 4 \bmod 7$ $\quad \Rightarrow \delta = 6 \Rightarrow 3$ первообразный корень по mod 7.

$3^5 = 243 \bmod 7 = 5 \bmod 7$

$3^6 = 729 \bmod 7 = 1 \bmod 7$

Пример $a = 5 \bmod 7$.

$5^1 = 5 \bmod 7$

$5^2 = 4 \bmod 7$

$5^3 = 125 \bmod 7 = 6 \bmod 7$

$5^4 = 625 \bmod 7 = 2 \bmod 7$ $\quad \Rightarrow \delta = 6 \Rightarrow 5$ является первообразным корнем по mod 7.

$5^5 = 3125 \bmod 7 = 3 \bmod 7$

$5^6 = 15625 \bmod 7 = 1 \bmod 7$

Пример

$8x = 2 \; mod \; 3$

$x = \left(8^{\varphi(3)-1} \cdot 2\right) \; mod \; 3$

$f(3) = (3 - 1) = 2$

$x = 16 \; mod \; 3$

$x = 1 \; (mod \; 3)$

Пример

$7x = 8 \; mod \; 15$

$x = ((-1)^{n-1} \cdot p_{n-1} \cdot b) \; mod \; m$

$15 = 7 \cdot 2 + 1$ $q_0 = 2$ $p_0 = 1$
$7 = 1 \cdot 7 + 0$ $q_1 = 7$ $p_1 = 7$
$x = ((-1)^1 \cdot 7 \cdot 8) mod\ 15\ = 14\ mod\ 15$

Пример

23 x = 42 mod 17
$17 = 23 \cdot 0 + 17$ $q_1 = 0$ $p_0 = 1$ $p_1 = 0$
$23 = 17 \cdot 1 + 6$ $q_2 = 1$ $p_2 = 1$
$17 = 6 \cdot 2 + 5$ $q_3 = 2$ $p_3 = 2$
$6 = 5 \cdot 1 + 1$ $q_4 = 1$ $p_4 = 3$
$5 = 1 \cdot 5 + 0$ $q_5 = 5$ $p_5 = 17$
$x = ((-1)^4 \cdot 3 \cdot 42) \bmod 17$
x = 7 (mod 17)

Пример

259 x = 179 mod 337
$337 = 259 \cdot 1 + 78$ $q_1 = 1$ $p_1 = 1$
$259 = 78 \cdot 3 + 25$ $q_2 = 3$ $p_2 = 4$
$78 = 25 \cdot 3 + 3$ $q_3 = 3$ $p_3 = 13$
$25 = 3 \cdot 8 + 1$ $q_4 = 8$ $p_4 = 108$
$8 = 1 \cdot 8 + 0$ $q_5 = 1$ $p_5 = 108 \cdot 8 + 13 = 877$
$x = ((-1)^4 \cdot 108 \cdot 179) \bmod 337$
x = 123 (mod 337)

3.4 Упражнения к практической работе

1 Найти обратный элемент (мультипликативную инверсию) с использованием РАЕ:

$33^{-1} \bmod 11$
$12^{-1} \bmod 17$
$132^{-1} \bmod 13$
$52^{-1} \bmod 13$
$532^{-1} \bmod 11$
$37^{-1} \bmod 13$
$62^{-1} \bmod 17$
$67^{-1} \bmod 19$

2Решить линейные сравнения через подходящие дроби
21x =42 mod 51
5x = mod 132

3x = 18 mod 48
25x = 58 mod 7
36x = 18 mod 12
13x = 69 mod 52
5x = 625 mod15
7x = 25 mod 19
7x = 8 mod 15
23 x =42 mod 17
259 x = 179 mod 337
111x = 75 mod 321

2Решить линейные сравнения с использованием функции Эйлера
13x = 7 mod 19
15x = 9 mod 27
15x = 5 mod 27
7x = 8 mod 15
5 x = 7 mod 11
6 x = 5 mod 13
7 x = 8 mod 15
6x = 8 mod 17
23 x =42 mod 17
259 x = 179 mod 337
113x = 75 mod 321

3.5 Контрольные вопросы

1.Что показывает функция Эйлера, как она рассчитывается?
2.Дать определение непрерывной и подходящий дробей.
3.Как рассчитываются непрерывные и подходящие дроби?
4.Укажите формулу решения линейного сравнения с помощью функции Эйлера.
5. Укажите формулу решения линейного сравнения с помощью подходящих дробей.

4 Практическая работа № 4. Решение системы линейных сравнений 1 степени с помощью Китайской теоремы об остатках

4.1 Постановка задачи

Цель работы:освоитьметод решения системы линейныхсравнений 1 степени с помощью китайской теоремы об остатках

Задание: научится решать систему линейные сравнений 1 степени:

4.2 Теоретические предпосылки

Решение системы линейных сравнений

$$\begin{cases} a_1 x \equiv b_1 \bmod m_1 \\ a_2 x \equiv b_2 \bmod m_2 \\ \quad \ldots \\ a_s x \equiv b_s \bmod m_s \end{cases}$$

Если каждое из этих сравнений имеет решение, тогда разрешив каждое линейное сравнение относительно x систему сравнений можно привести к следующему виду

$$\begin{cases} x_1 \equiv b_1 \bmod m_1 \\ x_2 \equiv b_2 \bmod m_2 \\ \quad \ldots \\ x_s \equiv b_s \bmod m_s \end{cases}$$

Китайская теорема об остатках

Суть теоремы: целое число можно восстановить по множеству его остатков от деления на числа из некоторого набора попарно взаимно простых чисел.

Теорема была доказана приблизительно в 100 году до н.э.

Впервые была упомянута в трактате китайского математика С. Цзы.

В 1247 г. до н.э. китайский математик ДжуШаоКвин вывел формулу для вычисления этого числа.

Китайская теорема об остатках

Пусть $m_1,\ldots m_k$ – попарно взаимно простые натуральные числа.

Тогда всякая система (*) имеет одно и только одно решение в $Z_{m1,\ldots mk}$

Пусть m_i , $1 \le I \le k$, – взаимно простые числа и $M = m_1 \cdot m_2 \cdot \ldots \cdot m_k$

Пусть a_i , $0 \le a_i \le m_i$, целые числа.

Введем обозначение $M_i = M/m_i$

Пусть y_i число, которое удовлетворяет системе сравнений

$M_i y_i \equiv 1 \bmod m_i$

При этих условиях система сравнений

$x \equiv a_i \bmod m_i$ имеет на интервале [0, M – 1] единственное решение, которое определяется формулой

$$x = a_1 y_1 M_1 + a_2 y_2 M_2 + \ldots + a_k y_k M_k$$

4.3 Примеры решения практических заданий

Решить систему сравнений:

$x \equiv a_1 \bmod 4,$

$x \equiv a_2 \bmod 5,$ где $m_1=4$, $m_2=5$, $m_3=7$.

$x \equiv a_3 \bmod 7,$

1) Определим число

$M = m_1 \cdot m_2 \cdot m_3 = 4 \cdot 5 \cdot 7 = 140$

2) Вычислим

$M_1 = M/m_1 = 140/4 = 35,$

$M_2 = M/m_2 = 140/5 = 28,$

$M_3 = M/m_3 = 140/7 = 20.$

3) Вычислим N_1, N_2, и N_3 из следующих сравнений:

$M_1 y_1 = 35 y_1 \equiv 1 \bmod 4,$

$M_2 y_2 = 28 y_2 \equiv 1 \bmod 5,$

$M_3 y_3 = 20 y_3 \equiv 1 \bmod 7.$

$y_1=3$; $y_2=2$; $y_3=6$

4) $x = (a_1 y_1 M_1 + a_2 y_2 M_2 + a_3 y_3 M_3 = (35 \cdot 3a_1 + 28 \cdot 2a_2 + 20 \cdot 6a_3) \bmod 140.$

4.4 Упражнения к практической работе

Значения a1, a2, a3 выбрать следующим образом: порядковый номер в списке + 3k, где k=1, 2, 3

$x \equiv a_1 \bmod 3,$

$x \equiv a_2 \bmod 5,$

$x \equiv a_3 \bmod 7,$

$2x \equiv a_1 \bmod 4,$

$x \equiv a_2 \bmod 5,$

$x \equiv a_3 \bmod 9,$

$3x \equiv a_1 \bmod 3,$

$x \equiv a_2 \bmod 5,$

$x \equiv a_3 \bmod 9,$

4 $x \equiv a_1 \mod 4$,
$x \equiv a_2 \mod 5$,
$x \equiv a_3 \mod 11$,

$5x \equiv a_1 \mod 4$,
$x \equiv a_2 \mod 7$,
$x \equiv a_3 \mod 11$,

$6x \equiv a_1 \mod 3$,
$x \equiv a_2 \mod 5$,
$x \equiv a_3 \mod 11$,

7 $x \equiv a_1 \mod 13$,
$x \equiv a_2 \mod 5$,
$x \equiv a_3 \mod 7$,

8 $x \equiv a_1 \mod 6$,
$x \equiv a_2 \mod 5$,
$x \equiv a_3 \mod 7$,

$9x \equiv a_1 \mod 4$,
$x \equiv a_2 \mod 6$,
$x \equiv a_3 \mod 7$,

10 $x \equiv a_1 \mod 4$,
$x \equiv a_2 \mod 5$,
$x \equiv a_3 \mod 8$,

$$\begin{cases} x = 8\ mod\ 17 \\ 2x = 12\ mod\ 29 \\ x = 4\ mod\ 11 \end{cases}$$

$$\begin{cases} x = 6\ mod\ 17 \\ 5x = 22\ mod\ 29 \\ x = 15\ mod\ 111 \end{cases}$$

$$\begin{cases} x = 17\ mod\ 19 \\ 7x = 12\ mod\ 19 \\ x = 5\ mod\ 11 \end{cases}$$

$$\begin{cases} x = 8\ mod\ 17 \\ 4x = 12\ mod\ 19 \\ x = 5\ mod\ 11 \end{cases}$$

$$\begin{cases} x = 6\ mod\ 15 \\ 8x = 11\ mod\ 18 \\ x = 7\ mod\ 11 \end{cases}$$

4.5 Контрольные вопросы

1. С какой целью применяется китайская теорема об остатках?
2. Сколько решений имеет система линейных первой степени?
3. Раскройте метод решения системы линейных сравнений первой степени с помощью китайской теоремы об остатках.
4. В каком случае система имеет решения?
5. Для чего применяется Китайская теорема об остатках?
6. Опишите алгоритм решения системы линейных сравнений первой степени с помощью КТО.

5 Практическая работа № 5. Диофантовы уравнения

5.1 Постановка задачи

Цель работы: изучить основные понятия и способы решения диофантовых уравнений.

Задание:

1) Научиться применять алгоритм быстрого возведения в степень по модулю.

2) научится решать диофантовы уравнения:

– частное решение;

– общие решения.

5.2 Теоретические предпосылки

1) Рассмотрим алгоритм быстрого возведения в степень по модулю бинарным методом

$a^b \bmod P$:

1. Представим показатель степени b в двоичной системе исчисления:

$b = (b_0 b_1 ... b_k)_2$ Например, $159 = 10011111_2$

2. Далее необходимо заполнить таблицу:

b	b_0	b_1	…	b_k
a	a_0	a_1	…	a_k

где $a_0 = a$, $a_{i+1} = \begin{cases} a_i^2 \bmod n, & \text{если } b_{i+1} = 0, \\ a_i^2 \cdot a \bmod n, & \text{если } b_{i+1} = 1 \end{cases}$ для $i \geq 0$.

Результатом возведения числа a в степень b по модулю станет последняя ячейка второй строки.

Пример

Возвести в степень по модулю:

$3^{177} \bmod 1003$

1	0	1	1	0	0	0	1
3	9	243	619	15	225	475	853

Ответ: $3^{177} \bmod 1003 = 853$

2) Линейные диофантовы уравнения

Пусть a, b, c - целые числа, $a \neq 0$. Рассмотрим уравнение вида:

$$ax + by = c \quad (**)$$

Нас будут интересовать только целочисленные решения.

Определение. Уравнение такого вида называется линейным диофантовым уравнением.

Определение. Алгебраическое уравнение с целыми коэффициентами, у которого отыскиваются целые или рациональные решения, называется диофантовым.

Этот тип уравнения либо не имеет решений, либо имеет бесконечное число решений.

Пусть d = НОД (a, b). Если d mod c <> 0, то уравнение не имеет решения. Если d mod c =0 (делится без остатка), то мы имеем бесконечное число решений.

Одно из них называется частным, остальные — общими.

Частное решение ax + by = c (**)

1. Преобразуем уравнение (**) к виду $a_1x + b_1y = c_1$, разделив обе части уравнения на d.
2. Найти x и y в равенстве $a_1x + b_1y = 1$, используя расширенный *алгоритм Евклида*.
3. *Частное решение*: $x_0 = (c/d)x$ и $y_0 = (c/d)y$

Общие решения

$x = x_0 - (b/d)\ k$ и $y = y_0 + (a/d)k$, где k — целое число

5.3 Примеры решения практических заданий

1) Возведение числа в степень по модулю

$4^{53} \bmod 11$

1	1	0	1	0	1
4	9	4	9	4	9

$4^{53} \bmod 11 = 9$

$2^{39} \bmod 29$

1	0	0	1	1	1
2	4	16	19	26	18

$2^{39} \bmod 29 = 18$

$3^{52} \bmod 17$

1	1	0	1	0	1
3	13	16	3	9	5

$3^{52} \bmod 17 = 5$

$5^{148} \bmod 37$

1	1	0	1	0	1	0	0
5	14	11	13	21	22	3	9

$5^{148} \bmod 37 = 9$

$2^{243} \bmod 5$

1	1	1	1	0	0	1	1
2	3	3	3	4	1	2	3

$2^{243} \bmod 5 = 3$

2) Решение диофантовыхуравнений

15x + 36y = 3
5x + 12y = 1
d = (15, 36) = 6
6 mod 1 = 0

i	a_i	x_i	y_i	q_i
0	5	1	0	-
1	12	0	1	5/12
2	0	1	-5/12	

Частные решения: x_0= 9/6 y_0= -5/12

1. 12x + 28y = 37

d = (12, 28) = 4 cmodd = 1 =>Нет решений

2. 12x + 28y = 36

d = (12, 28) = 4 cmodd = 0 =>бесконечное число решений
3x + 7y = 9

PAE:

i	a_i	x_i	y_i	q_i
0	3	1	0	-
1	7	0	1	0
2	3	1	0	2
3	1	2	1	3
4	0			

x_0 = -18 y_0=9
x = -18 -7k
y = 9 + 3k

3) Решить систему линейных сравнений с помощью Китайской теоремы об остатках

Решить систему КТО:

$$\begin{cases} x = 8 \, mod \, 17 \\ 7x = 12 \, mod \, 19 \\ x = 5 \, mod \, 11 \end{cases}$$

7x = 12 mod 19
19 = 7·2 +5

7 = 5·1 +2
5 = 2·2 +1
2 = 1·2 + 0 $p_3 = 8$
$x = (-1)^3 \cdot 8 \cdot 12 \bmod 19$
x = 18 mod 19
(17; 19) = 1 (17; 11) = 1 (11;19) = 1
M = 17·19·11 = 3553
M_1= 3553 / 17 = 209
M_2 = 3553 / 19 = 187
M_3 = 3553 / 11 = 323

$$\begin{cases} M_1 y_1 = 1 \, mod \, m_1 \\ M_2 y_2 = 1 \, mod \, m_2 \\ M_3 y_3 = 1 \, mod \, m_3 \end{cases}$$

$$\begin{cases} 209 \, y_1 = 1 \, mod \, 17 \\ 187 \, y_2 = 1 \, mod \, 19 \\ 323 \, y_3 = 1 \, mod \, 11 \end{cases}$$

17 = 209 · 0 + 17 $p_0 = 1$ $p_1 = 0$
209 = 17·12 + 5 $p_2 = 1$
17 = 5·3 + 2 $p_3 = 1$
5 = 2·2 +1 $p_4 = 7$
2 = 1·2 + 0
$y_1 = (-1)^4 \cdot 7 \cdot 1 \bmod 17$
y_1 = 7 mod 17
19 = 187 · 0 + 19 $p_0 = 1$ $p_1 = 0$
187 = 19 · 9 + 16 $p_2 = 1$
19 = 16 · 1 + 3 $p_3 = 1$
16 = 3 · 5 + 1 $p_4 = 6$
3 = 1 · 3 + 0
y_2 = 6 mod 19
11 = 323 · 0 + 11 $p_0 = 1$ $p_1 = 0$
323 = 11 · 29 + 4 $p_2 = 1$
11 = 4 · 2 + 3 $p_3 = 2$
4 = 3 · 1 + 1 $p_4 = 3$
3 = 1 · 3 + 0
y = 3 mod 11
Y = (8·7·209 + 18·19·187 + 5·3·323) mod 3553 = 2337

5.4 Упражнения к практической работе

1Возвести в степень по модулю
5^{177}mod 103

$3^{17} \bmod 51$

$7^{77} \bmod 1001$

$3^{51} \bmod 203$

$5^{157} \bmod 111$

$7^{155} \bmod 1003$

2 Диофантово уравнение
$17x + 16y = 3k$
$15x + 26y = 2k$
$11x + 46y = 5k$
$13x + 38y = 7k$
k – порядковый номер в списке.

5.5 Контрольные вопросы

1. С какой целью необходимо применять понижение степени?
2. Раскройте суть возведения в степень по модулю бинарным способом?
3. Раскройте алгоритм решения диофантово уравнения.
4. Сколько решений имеет диофантово уравнение?

6 Практическая работа № 6. Символ Якоби и Лежандра

6.1 Постановка задачи

Цель работы: изучить основные понятия и способы нахождения символа Якоби и символа Лежандра

Задание: научится находить символы Якоби и Лежандра.

6.2 Теоретические предпосылки

Сравнения второй степени

Из сравнений степени n>1 рассматриваем простейшие – двучленные сравнения:

$$x^n \equiv a(\mathrm{mod} p);\ (a,m)=1$$

Если сравнение (1) имеет решения, то а называется вычетом степени n по модулю m.

Если n=2 вычеты и невычеты называются квадратичными

Если n=3 вычеты и невычеты называются кубическими

Если n=4 вычеты и невычеты называются биквадратными.

Рассмотрим более подробно двучленные сравнения второй степени:

$$x^2 \equiv a(\mathrm{mod} p);\ (a,p)=1$$

Если а – квадратичный вычет по модулю р, то сравнение имеет 2 решения.

Действительно, если а– квадратичный вычет, то сравнение имеет, по крайней мере, одно решение $x \equiv x_1(\mathrm{mod} p)$, тогда ввиду $(-x_1)^2=x_1^2$, то же сравнение имеет второе решение $x \equiv -x_1(\mathrm{mod} p)$, которое отлично от первого, так как из $x_1 \equiv -x_1(\mathrm{mod} p)$ было бы $2x_1 \equiv 0(\mathrm{mod} p)$, что невозможно в виду $(2,p) = (x_1,p) = 1$

Вывод: Двумя решениями исчерпываются все решения сравнения, так сравнение второй степени более двух решений иметь не может.

Приведенная система вычетов по модулю р состоит из квадратичных $\frac{p-1}{2}$ вычетов, сравнимых с числами:

$$1^2, 2^2, 3^2, \ldots \left(\frac{p-1}{2}\right)^2$$

и $\frac{p-1}{2}$ квадратичных невычетов

Действительно, среди вычетов приведенной системы вычетов по модулю р квадратичными вычетами являются те и только те, которые сравнимы с квадратами чисел (приведенной системы вычетов), то есть числами

$$-\frac{p-1}{2}, \ldots, -2, -1, 1, 2, \ldots, \frac{p-1}{2}$$

При этом числа по модулю рне сравнимы

Символ Лежандра

Определяется для всех а, не делящихся на р.

Задается равенством $\left(\frac{a}{p}\right)=1$ если а квадратичный вычет по модулю р, и равенством $\left(\frac{a}{p}\right)=-1$ если а квадратичный невычет по модулю р,

Вычислить символ Лежандра и таким путем определить, является ли а квадратичными вычетом или невычетом по модулю р позволяет критерий**Эйлера (теорема):**

При а, не делящемся на р, имеем

$$a^{\frac{p-1}{2}}=\left(\frac{a}{p}\right)(\mathrm{mod}\ p)$$

Свойства символа Лежандра

Если $a\equiv a_1(\mathrm{mod} p)$, то $\left(\frac{a}{p}\right)=\left(\frac{a_1}{p}\right)$

Действительно, $1=1^2$, следовательно $\left(\frac{1}{p}\right)=1$ - квадратичный вычет

Следствие из теоремы при а=-1 $\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$

Следствие $\left(\frac{a\cdot b\cdot\ldots\cdot l}{p}\right)=\left(\frac{a}{p}\right)\cdot\left(\frac{b}{p}\right)\cdot\ldots\cdot\left(\frac{l}{p}\right)$ $\left(\frac{a\cdot b^2}{p}\right)=\left(\frac{a}{p}\right)$

$$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}},$$

Если р и q простые нечетные, то (закон взаимности квадратичных вычетов)

$$\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{p}{q}\right)$$

Символ Якоби

Обобщение символа Лежандра

Пусть Р – нечетное, большее единицы, и $P=p_1p_2\ldots p_r$ – разложение его на простые сомножители. Пусть (a,P)=1, тогда символ Якоби определяется равенством

$$\left(\frac{a}{P}\right)=\left(\frac{a}{p_1}\right)\cdot\left(\frac{a}{p_2}\right)\cdot\ldots\cdot\left(\frac{a}{p_r}\right)$$

Свойства символа Якоби

Если a≡a$_1$(modp), то $\left(\frac{a}{P}\right)=\left(\frac{a_1}{P}\right)$, *если* $a \equiv a_1 (\mathrm{mod}\, P)$

$\left(\frac{1}{P}\right)=1$

$\left(\frac{-1}{P}\right)=(-1)^{\frac{P-1}{2}}$

$\left(\frac{a\cdot b\cdot \ldots \cdot l}{P}\right)=\left(\frac{a}{P}\right)\cdot\left(\frac{b}{P}\right)\cdot \ldots \cdot\left(\frac{l}{P}\right)$

Следствие $\left(\frac{a\cdot b^2}{P}\right)=\left(\frac{a}{P}\right)$ $\left(\frac{2}{P}\right)=(-1)^{\frac{P^2-1}{8}}$,

Если P и Qпростые нечетные и взаимно простые, то

$\left(\frac{Q}{P}\right)=(-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}\left(\frac{P}{Q}\right)$

6.3 Примеры решения практических заданий

1.Определить является ли 5 квадратичным вычетом по модулю 29

$$a^{\frac{p-1}{2}}=\left(\frac{a}{p}\right)(\mathrm{mod}\ p)=5^{\frac{29-1}{2}}=\left(\frac{5}{29}\right)(\mathrm{mod}\ 29)=5^{14}\ \mathrm{mod}\ 29=1$$

Следовательно 5 квадратичный вычет по модулю 29 и сравнение $x^2\equiv 5(\mathrm{mod}\ 29)$ имеет два решения

2. Определить является ли 3 квадратичным вычетом или невычетом по модулю 29.

Следовательно 3 квадратичный невычет по модулю 29 и сравнение $x^2\equiv 3(\mathrm{mod}\ 29)$ решение не имеет

$$3^{14}=\left(\frac{3}{14}\right)(\mathrm{mod}\ 29)=28(\mathrm{mod}\ 29)=-1(\mathrm{mod}\ 29)$$

Рассматривая символ Лежандра как частный случай символа Якоби и пользуясь свойствами можно вычислить символ Лежандра быстрее, чем по критерию Эйлера (теореме)

$$\left(\frac{219}{383}\right)=(-1)^{\frac{219-1}{2}\cdot\frac{383-1}{2}}\left(\frac{383}{219}\right)=-\left(\frac{383}{219}\right)=-\left(\frac{164}{219}\right)=-\left(\frac{41}{219}\right)=$$

$$\left(\frac{219}{41}\right)=-\left(\frac{14}{41}\right)=-\left(\frac{2}{41}\right)\cdot\left(\frac{7}{41}\right)=-\left(\frac{7}{41}\right)=-\left(\frac{41}{7}\right)=-\left(\frac{-1}{7}\right)=1$$

Следовательно, рассмотренное сравнение имеет два решения.

3 Вычислить символ Якоби или Лежандра и указать число решений для сравнения:

$$\frac{29}{163}=(-1)^{\frac{163-1}{2}\cdot\frac{29-1}{2}}\left(\frac{163}{29}\right)=(-1)^{81\cdot14}\left(\frac{163}{29}\right)=\frac{163}{29}=\frac{18}{29}=\frac{3}{29}\cdot\frac{3}{29}\cdot\frac{2}{29}$$
$$=1\cdot\frac{2}{29}=(-1)^{\frac{29^2-1}{8}}=(-1)^{105}=-1$$

Решений нет.

4Вычислить символ Якоби или Лежандра и указать число решения для сравнения.

$$\frac{11}{29}$$

$$\frac{11}{29}=\frac{29}{11}\cdot(-1)^{\frac{29-1}{2}\cdot\frac{11-1}{2}}=\frac{7}{11}=(1)^{\frac{11-1}{8}}=1$$

Ответ:является квадратичным вычетом.

5 Вычислить символ Якоби или Лежандра и указать число решения для сравнения.

$$\frac{13}{23}$$

оба числа простые вычисляем символ Лежандраиспользуя два свойства

$$\text{если a}<n\text{, то }\frac{\mathrm{a}}{\mathrm{n}}=(-1)^{\frac{\mathrm{a}-1}{2}\cdot\frac{\mathrm{n}-1}{2}}\frac{\mathrm{n}}{\mathrm{a}};$$

если а четное, то

$$\frac{\mathrm{a}}{\mathrm{n}}=\frac{\mathrm{a}/2}{\mathrm{n}}\cdot(-1)^{\frac{\mathrm{n}^2-1}{8}};$$

$$\frac{13}{23}=\frac{23}{13}\cdot(-1)^{\frac{23-1}{2}\cdot\frac{13-1}{2}}=\frac{23}{13}=\frac{10}{13}=\left(\frac{5}{13}\right)\cdot(-1)^{\frac{13-1}{2}}=\frac{5}{13}=\frac{13}{5}=$$
$$=\frac{3}{5}\cdot(-1)^{\frac{3-1}{2}\cdot\frac{5-1}{2}}=\frac{3}{5}=\frac{5}{3}=\frac{2}{3}=(-1)^{\frac{9-1}{8}}=-1$$

Ответ: Решений нет.

6Вычислить символ Якоби или Лежандра и указать число решения для сравнения.

$$\frac{15}{123}$$

a=15 – нечетное, составное
p=123 – нечетное, составное

Вычисляем символ Лежандра:

$$\frac{15}{123}=\frac{15}{41}\cdot\frac{5}{3}$$

$$\frac{15}{41}=\left(\frac{3}{41}\right)\cdot\left(\frac{5}{41}\right)=\frac{41}{3}\cdot(-1)^{\frac{41-1}{2}\cdot\frac{5-1}{2}}=\left(\frac{41}{3}\right)\cdot\left(\frac{41}{5}\right)\cdot\left(\frac{2}{3}\right)\cdot\left(\frac{1}{5}\right)=(-1)^{\frac{3^2-1}{8}}\cdot 1=-1$$

$\frac{15}{3}$ – делится нацело, следовательно, ответ =0

-1·0=0
Ответ: 0

7Вычислить символ Якоби или Лежандра и указать число решения для сравнения:

$$\frac{5}{29}$$

Решение: $\frac{5}{29}=(-1)^{\frac{5-1}{2}\cdot\frac{29-1}{2}}\cdot\left(\frac{29}{5}\right)=(-1)^{2\cdot 14}\cdot\left(\frac{29}{5}\right)=\frac{29}{5}=\frac{4}{5}=1$

$5^{\frac{29-1}{2}} \bmod 29$;
$5^{14} \bmod 29 = 1 \Rightarrow 2$ решения;
$X^2 \equiv 5 \bmod 29$ имеет 2 решения.
Ответ: имеет 2 решения.

6.4 Упражнения к практической работе

Вычислить символ Якоби или Лежандра и указать число решения для сравнения

Вариант 1	**Вариант 2**	**Вариант 3**	**Вариант 4**
$\frac{15}{123}$	$\frac{5}{29}$	$\frac{11}{29}$	$\frac{5}{31}$
Вариант 5	**Вариант 6**	**Вариант 7**	**Вариант 8**
$\frac{105}{37}$	$\frac{29}{163}$	$\frac{15}{129}$	$\frac{13}{143}$
Вариант 9	**Вариант 10**	**Вариант 11**	**Вариант 12**
$\frac{15}{17}$	$\frac{15}{123}$	$\frac{13}{23}$	$\frac{15}{113}$
Вариант 13	**Вариант 14**	**Вариант 15**	**Вариант 16**
$\frac{15}{23}$	$\frac{14}{237}$	$\frac{17}{123}$	$\frac{15}{47}$

6.5 Контрольные вопросы

1. Дайте определения сравнению второй степени? Сколько имеет решений.
2. Квадратичный вычет по модулю.
3. Что представляет собой символ Лежандра?
4. Что представляет собой символ Якоби?
5. Как найти символ Лежандра, Якоби? Критерий Эйлера.
6. Свойства символа Лежандра, Якоби. Для чего и как применяются?

7 Практическая работа № 7. Решение квадратичных сравнений

7.1 Постановка задачи

Цель работы: изучить основные понятия и методы решения квадратичных сравнений

Задание: научится решать квадратичные сравнения.

7.2 Теоретические предпосылки

Извлечение квадратного корня из квадратичного вычета по простому модулю

Пусть p нечетное простое число, a – целое число, взаимно простое с p

Если сравнение $x^2 \equiv a \pmod p$ разрешимо, то выполнены следующие утверждения

1. если $p \equiv 3 \pmod 4$, то $x \equiv a^{\frac{p+1}{4}} \pmod p$

2. если $p \equiv 5 \pmod 8$, то

$$\text{если} \quad a^{\frac{p-1}{4}} \equiv 1 \pmod p, \quad \text{то} \quad x \equiv a^{\frac{p+3}{8}} \pmod p$$

$$\text{если} \quad a^{\frac{p-1}{4}} \equiv -1 \pmod p, \quad \text{то} \quad x \equiv 2a(4a)^{\frac{p-5}{8}} \pmod p$$

3. если $p \equiv 1 \pmod 4$, то решается методом Шенкса-Тоннели (не рассматривается в рамках данных методических рекомендаций).

Извлечение квадратного корня по составному модулю. Если n(p) произведение простых сомножителей можно представить следующим алгоритмов в виде рисунка 7.1:

$$x^2 = a \pmod n, \Rightarrow \begin{cases} x^2 \equiv a_1 \bmod p_1 \\ x^2 \equiv a_1 \bmod p_1 \\ \quad \ldots \\ x^2 \equiv a_k \bmod p_k \end{cases} \Rightarrow \begin{cases} x^2 \equiv \pm b_1 \bmod p_1 \\ x^2 \equiv \pm b_1 \bmod p_1 \\ \quad \ldots \\ x^2 \equiv \pm b_k \bmod p_k \end{cases}$$

$n = p_1 p_2 \ldots p_k$

Рисунок 7.1 —Алгоритм решения квадратичного сравнения

Решение:

1. Исходное сравнение раскладывается в систему нескольких квадратичных сравнений по простому модулю. Если они разрешимы, находим

решение для каждого.

2. Решаем отдельно системы для всех возможных сочетаний предыдущих решений с использованием КТО

3. Квадратичные сравнения по составному модулю.

Рассмотрим сравнение вида $x^2 \equiv a \pmod{p^\alpha}$, где p – простое нечетное число. Решение этого сравнения можно отыскать, решив сравнение $x^2 \equiv a \pmod{p}$. Причем сравнение $x^2 \equiv a \pmod{p^\alpha}$ будет иметь два решения, если a является квадратичным вычетом по модулю p.

Рассмотрим теперь сравнение вида $x^2 \equiv a \pmod{2^\alpha}$. Такое сравнение не всегда имеет два решения. Для такого модуля возможны случаи:

1 $\alpha=1$. Тогда сравнение имеет решение только тогда, когда $a \equiv 1 \pmod 2$, и решением будет $x \equiv 1 \pmod 2$ (одно решение).

2 $\alpha=2$. Сравнение имеет решения только тогда, когда $a \equiv 1 \pmod 4$, и решением будет $x \equiv \pm 1 \pmod 4$ (два решения).

3 $\alpha \geq 3$. Сравнение имеет решения только тогда, когда $a \equiv 1 \pmod 8$, и таких решений будет четыре. Сравнение $x^2 \equiv a \pmod{2^\alpha}$ при $\alpha \geq 3$ решается так же, как сравнения вида $x^2 \equiv a \pmod{p^\alpha}$, только в качестве начального решения выступают решения по модулю 8: $x \equiv \pm 1 \pmod 8$ и $x \equiv \pm 3 \pmod 8$. Их следует подставить в сравнение по модулю 16, затем по модулю 32 и т. д. вплоть до модуля 2^α.

Теперь рассмотрим сравнение общего вида: $x^2 \equiv a \pmod m$, $(a,m)=1, m = 2^\alpha p_1^{\alpha 1} p_2^{\alpha 2} \dots p_k^{\alpha k}$ - каноническое разложение модуля m.

Данному сравнению равносильна система:

$$\begin{cases} x^2 \equiv a (mod 2^\alpha) \\ x^2 \equiv a (mod p_1^{\alpha 1}) \\ x^2 \equiv a (mod p_2^{\alpha 2}) \\ \dots \\ x^2 \equiv a (mod p_k^{\alpha k}) \end{cases}$$

Если каждое сравнение этой системы разрешимо, то разрешима и вся система. Найдя решение каждого сравнения этой системы, мы получим систему сравнений первой степени, решив которую по китайской теореме об остатках, получим решение исходного сравнения. При этом количество различных решений исходного сравнения (если оно разрешимо) есть 2^k, если $\alpha=1$, 2^{k+1}, если $\alpha=2$, 2^{k+2}, если $\alpha \geq 3$.

7.3 Примеры решения практических заданий

1 Определить количество решений и найти их для сравнения второй степени:

а) $x^2 = 5 mod 17$

$$\frac{5}{17} = (-1)^{\frac{5-1}{2}\cdot\frac{17-1}{2}} \left(\frac{17}{5}\right) = (-1)^{2\cdot 8} \left(\frac{17}{5}\right) = \frac{17}{5} = \frac{2}{5} = (-1)^{\frac{5^2-1}{8}} = (-1)^{\frac{25-1}{8}} = -1$$

Решений нет

б)$x^2 = 41 mod 64$

$$\frac{41}{64} = \left(\frac{41}{2}\right)^6 = 1$$

41=1mod8 =>уравнение имеет 4 решения

mod8: $x = \pm 1 mod 8$

$x = \pm 3 mod 8$

$x = \pm(1 + 4t_1)$

$$mod 16: x^2 = 9 mod 16$$

$(1 + 4t_1)^2 = 9 mod 16$

$1 + 8t_1 + 16{t_1}^2 = 9 mod 16$

$8t_1 = 8 mod 16$

$t_1 = 1 mod 2$

$x = 1 + 4(1 + 2t_2) = 1 + 4 + 8t_2 = 5 + 8t_2$

$mod 32: x^2 = 41 mod 32$

$(5 + 8t_2)^2 = 41 mod 32$

$25 + 80t_2 + 64{t_2}^2 = 9 mod 32$

$80t_2 = -16 mod 32$

$80t_2 = 16 mod 32$

$16t_2 = 16 mod 32$

$t_2 = 1 mod 32$

$x = \pm(5 + 8t_2) = \pm\big(5 + 8(1 + 32t_3)\big) = \pm(5 + 8 + 256t_3) = \pm(13 + 256t_3)$

$mod 64: x^2 = 41 mod 64$

$(13 + 256t_3)^2 = 41 mod 64$

$169 + 6656t_3 + 65536{t_3}^2 = 41 mod 64$

$$6656t_3 = -128 mod 64$$

$6656t_3 = 0 mod 64$

$t_3 = 0 mod 64$

$x = \pm\big(13 + 256(0 + 64t_4)\big) = \pm(13 + 16384t_4) = \pm 13 mod 64$

2Определить количество решений и найти их для сравнения второй степени.

a) $x^2 = 3 \bmod 19$

$$\frac{3}{19} = \frac{19}{13} \cdot (-1)^{\frac{3-1}{2} \cdot \frac{19-1}{2}} = \frac{1}{3} \cdot (-1) = -\frac{1}{3} = -1$$

Ответ: Решений нет.

b) $x^2 = 3 \bmod 277$

$$\frac{3}{277} = \frac{277}{3} \cdot (-1)^{\frac{3-1}{2} \cdot \frac{277-1}{2}} = \frac{1}{138} \cdot (1) =$$

$1 -$ 2 Решения $\rightarrow$x=$3^{\left(\frac{277+3}{8}\right)} \mathrm{mod} 277 = 147$

Ответ: x=$\pm 147 \mathrm{mod} 277$

3 Определить количество решений и найти их для сравнения второй степени.

c) $x^2 = 11 \bmod 13$

$\frac{11}{13}$, оба числа простые, вычислим символ Лежандра, используя свойство

если a $< n$, то $\frac{a}{n} = (-1)^{\frac{a-1}{2} * \frac{n-1}{2}} \frac{n}{a}$;

$\frac{11}{13} = \frac{13}{11} \cdot (-1)^{\frac{13-1}{2} \cdot \frac{11-1}{2}} = \frac{13}{11} = \frac{2}{11} \cdot (-1)^{\frac{121-1}{8}} = (-1)^{15} = -1$ – Решений нет

Ответ: Решений нет.

d) $x^2 = 7 \bmod 55$

Решение.

Решение производится методом извлечение квадратного корня по составному модулю. Если n(p) произведение простых сомножителей.

$x^2 = 7 \bmod 55$

$55 = 11 \cdot 5$

Составляем систему квадратичных сравнений:

$$\begin{cases} x^2 = \pm 7 \bmod 11 \\ x^2 = \pm 7 \bmod 5 \end{cases}$$

Проверяем, разрешимо ли каждое квадратичное сравнение с помощью символа Лежандра.

$\frac{7}{11}$, оба числа простые, вычисляем символ Лежандра, используя свойства

если a $< n$, то $\frac{a}{n} = (-1)^{\frac{a-1}{2} \cdot \frac{n-1}{2}} \cdot \frac{n}{a}$;

$\frac{2}{n} = (-1)^{\frac{n-1}{8}}$;

$$\frac{7}{11} = \frac{11}{7} \cdot (-1)^{\frac{7-1}{2} \cdot \frac{11-1}{2}} = \frac{4}{7} = \frac{{}^{4}/_{2}}{7} \cdot (-1)^{\frac{7^2-1}{8}} = (-1)^{\frac{7^2-1}{8}} \cdot (-1)^{\frac{7^2-1}{8}} = 1$$

Есть два решения.

$\frac{7}{5}$, оба числа простые, вычесляем символ Лежандра, используя свойство

$\frac{2}{n} = (-1)^{\frac{n-1}{8}}$

Находим:

$\frac{2}{5} = (-1)^{\frac{25-1}{8}} = -1$ - Решений нет

Из этого следует, что:

$\frac{7}{55} = 1 \cdot (-1) = -1$ - Решений нет

Ответ: Решений нет.

4Определить количество решений и найти их для сравнения второй степени:

$X^2 = 3 \bmod 31$

$X^2 = 59 \bmod 125$

Решение: $X^2 = 3 \bmod 31 = (-1)^{\frac{32-1}{2} \cdot \frac{3-1}{2}} \cdot (\frac{32}{3}) = -(\frac{31}{3}) = -\frac{1}{3} = -1$

Символ Лежандра $= -1 \Rightarrow$ решения нет.

$X^2 = 59 \bmod 125$

$5^3 = 125$

$\frac{59}{4} = \frac{4}{5} = (\frac{2}{5})^2 = 1$

$X^2 \equiv 59 \bmod 5$

$X^2 \equiv 4 \bmod 5$

$X \equiv \pm 2 \bmod 5$

$X = \pm(2 + 5t_1)$

$X^2 = 59 \bmod 25$

$(2 + 5t_1)^2 = 9 \bmod 25$

$4 + 20t_1 + 25t_1^2 = 9 \bmod 25$

$20t_1 = 5 \bmod 25$

$4t_1 = 1 \bmod 5$

$t_1 = -1 \bmod 5$

$X = \pm(2 + 5t_1) = \pm(2 + 5(-1 + 5t_2) = \pm(2 + 25t_2 - 5) = \pm(25t_2 - 3)$

$X^2 = 59 \bmod 125$

$(25t_2 - 3)^2 = 59 \bmod 125$

$625 - 150t_2 + 9 = 59 \bmod 125$

$-25t_2 \equiv 50 \bmod 25$

$t_2 \equiv -2 \bmod 5$

$X = \pm(25t_2 - 3) = \pm(25(-2 + 5t_3) - 3) = \pm(-53 + 125t_3)$

$X = \pm 53 \bmod 125$

Ответ: $X = \pm 53 \bmod 125$

7.4 Упражнения к практической работе

Определить количество решений и найти их для сравнения второй степени по вариантам (таблица 7.1):

Таблица 7.1 – Выбор вариантов для выполнения упражнений

Вариант 1	Вариант 2	Вариант 3	Вариант 4
X^2=4mod19 x2=91mod243	X^2=3mod31 x2=59mod125	x2=3mod19 x2=3mod277	x2=5mod19 x2=2mod97
Вариант 5	Вариант 6	Вариант 7	Вариант 8
X^2=2mod17 x2=145mod256	X^2=5mod17 x2=41mod64	X^2=7mod17 x2=11mod353	X^2=6mod17 x2=2mod311
Вариант 9	Вариант 10	Вариант 11	Вариант 12
X^2=4mod13 x2=13mod33	X^2=7mod13 x2=7mod33	X^2=11mod13 x2=7mod55	X^2=5mod13 x2=9mod77
Вариант 13	Вариант 14	Вариант 15	Вариант 16
X^2=4mod29 x2=36mod77	X^2=5mod29 x2=429mod563	X^2=11mod23 x2=226mod563	X^2=9mod23 x2=36mod77

7.5 Контрольные вопросы

1. Общий вид сравнения второй степени. Когда и сколько имеет решений?
2. Общий способ извлечения квадратного корня из квадратичного вычета по простому модулю.
3. Способы извлечения квадратного корня по составному модулю.

8 Практическая работа № 8. Полиномы. Поля Галуа

8.1 Постановка задачи

Цель работы: изучить основные понятия и методы решения квадратичных сравнений

Задание: научится решать квадратичные сравнения.

8.2 Теоретические предпосылки

Конечные поля

В криптографии используются только конечные поля. **Конечное поле** — поле с конечным числом элементов — является очень важной структурой в криптографии. Галуа показал что поля, чтобы быть конечными, должны иметь число элементов p^n, где p — простое, а n — положительное целое число. Конечные поля обычно называют **полями Галуа** и обозначают как GF(p^n).

Поле Галуа, GF(p^n), — конечное поле с p^n элементами.

Поля GF (p)

Когда n = 1, мы имеем поле GF (p). Это поле может быть множеством Z_p, (0, 1, …p–1) с двумя арифметическими операциями (сложение и умножение). Любой элемент в этом множестве имеет аддитивную *инверсию*, и элементы, отличные от нуля, имеют мультипликативную*инверсию*(мультипликативная*инверсия*для0отсутствует.

Очень общее поле в этой категории — GF (2) с множеством {0,1} и двумя операциями, сложением и умножением, как показано на рисунке 3.

{0,1}
+ ×

+	0	1
0	0	1
1	1	0

Сложение

×	0	1
0	0	0
1	0	1

Умножение

a	0	0
-a	1	1

a	0	1
a^{-1}	-	1

Инверсия

Рисунок 8.1—Поле GF

Есть несколько моментов, которые следует отметить в определении этого поля. Первый: множество имеет только два элемента, которые являются двоичными цифрами или битами (0 и 1). Второй: операция сложения — фактически ИСКЛЮЧАЮЩЕЕ ИЛИ (XOR), операция, которую мы используем с двумя двоичными цифрами. Третий: операция умножения — AND, операция, которую мы используем с двумя двоичными цифрами. Четвертый: сложение и операции вычитания — те же самые (операцияXOR). Пятый: умножение и операции деления — те же самые (ОПЕРАЦИЯ AND).

Сложение/вычитание в GF(2) — операция ИСКЛЮЧАЮЩЕЕ ИЛИ (XOR); умножение/деление — ОПЕРАЦИЯ И (AND).

Полиномы

Хотя мы можем непосредственно определить правила для операций сложения и умножения слов из двух бит, которые удовлетворяют свойства в $GF(2^n)$, проще работать с полиномиальным степени n–1 побитным представлением слов. **Полиномиальное** выражение степени n – 1 имеет форму:

$$f(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots\ldots + a_1x^1 + a_0x^0 \qquad (8.1)$$

где x^i назван термином « i -тый элемент», а a_i называется коэффициентом i - того элемента. Хотя мы знаем полиномы в алгебре, но при представлении n -битовых слов полиномами необходимо следовать некоторым правилам:

− степень x определяет позицию бита в n -битовых слов. Это означает, что крайний левый бит находится в нулевой позиции (связан с x^0), самый правый бит находится в позиции n–l (связан с x^{n-l});

− коэффициенты сомножителей определяют значение битов. Каждый бит принимает только значение 0 или 1, поэтому наши полиномиальные коэффициенты могут иметь значение 0 или 1.

Операции

Обратите внимание, что любая операция на полиномах фактически включает две операции: операции И коэффициентов двух полиномов. Другими словами, мы должны определить два поля: одно для коэффициентов и одно для полиномов. Коэффициенты равны 0 или 1 ; для этой цели мы можем использовать GF(2) -поле. Для полиномов нам нужно поле $GF(2^n)$, которое мы коротко обсудим ниже.

Полиномы, представляющие n-битовые слова, используют два поля: GF(2) и $GF(2^n)$.

Модуль

Перед определением операций на полиномах мы должны поговорить о полиномах-модулях. Сложение двух полиномов никогда не создает полином, выходящий из множества. Однако умножение двух полиномов может создать полином со степенью большей, чем n – 1. Это означает, что мы должны делить результат на модуль и сохранять только остаток, как мы сделали в модульной арифметике. Для множеств полиномов в $GF(2^n)$ группа полиномов степени n определена как модуль. Модуль в этом случае действует как полиномиальное простое число. Это означает, что никакие полиномы множества не могут делить этот полином. Простое полиномиальное число не может быть разложено в полиномы со степенью меньшей, чем n. Такие полиномы называются неприводимые полиномы. Таблица 1 показывает примеры полиномов 1-5 степеней.

Для каждого значения степени часто есть более чем один неразлагаемый полином, — это означает, что когда мы определяем $GF(2^n)$, мы должны объявить, какой неприводимый полином мы используем как модуль (в таблице 8.1 приведен список некоторых неприводимых полиномов).

Таблица 8.1- Список неприводимых полиномов

Степень	Неприводимый полином
1	$(x+1)x$
2	(x^2+x+1)
3	$(x^3+x^2+1)(x^3+x+1)$
4	$(x^4+x^3+x^2+x+1)(x^4+x^3+1)(x^4+x+1)$
5	$(x^5+x^2+1)(x^5+x^3+x^2+x+1)(x^5+x^4+x^3+x+1)(x^5+x^4+x^3+x^2+1)(x^5+x^4+x^2+x+1)$

Сложение

Теперь определим операцию сложения для полиномов с коэффициентом в GF(2). Операция сложения очень простая: мы складываем коэффициенты соответствующих элементов полинома в поле GF(2). Обратите внимание, что сложение двух полиномов степени $n - 1$ всегда дает полином со степенью $n - 1$ — это означает, что мы не должны использовать вычитание из модуля их результата.

Аддитивный нейтральный элемент — тождество. Аддитивный нейтральный элемент полинома — нулевой полином (полином со всеми коэффициентами, равными нулю), потому что, прибавляя этот полином к самому себе, в результате получаем нулевой полином.

Аддитивная инверсия полинома с коэффициентами в GF(2) — сам полином. Это означает, что операция вычитания та же самая, что и операция сложения.

Сложение и операции вычитания на полиномах — та же самая операция.

Умножение

Умножение в полиномах — сумма умножения каждого элемента одного полинома с каждым элементом второго полинома. Однако необходимо отметить три особенности.

Первая: умножение коэффициента проводится в поле GF(2).

Вторая: умножение x^i на x^j дает результат x^{i+j}.

Третья: умножение может создать элементы со степенью большей, чем n–1, и это означает, что результат должен быть уменьшен с использованием полинома-модуля.

Сначала покажем, как умножить два полинома согласно вышеупомянутому определению. Позже будет дан более эффективный алгоритм, который может использоваться компьютерной программой.

Мультипликативная инверсия.

Поиск мультипликативной инверсии требует привлечения расширенного алгоритма Евклида. Алгоритм Евклида должен быть применен к модулю и полиному, выполнение алгоритма является таким же, как и для целых чисел.

8.3 Примеры решения практических заданий

1 Для каждого из слов найти полиномы, которые представляют эти слова.
00011
Полином: $0x^7 + 0x^6 + 0x^5 + 0x^4 + 0x^3 + 0x^2 + 1x^1 + 1x^0$
Первое упрощение: $1x^1 + 1x^0$
Второе упрощение: *x+1*

Ответ: *P=x+1*

2Для каждого из слов найти полиномы, которые представляют эти слова:

101111

$$x^5 + 0 * x^4 + x^3 + x^2 + x^1 + 1$$
$$x^5 + x^3 + x^2 + x^1 + 1$$

3 Найти сумму и произведение двух полиномов по модулю, найти мультипликативную инверсию для одного из чисел в поле Галуа:

17h = 10111 $x^4 + x^2 + x^1 + 1$
53h = 1010011 $x^6 + x^4 + x^1 + 1$

a) $(x^4 + x^2 + x + 1) \oplus (x^6 + x^4 + x + 1) = x^6 + x^4 + x^2$

b) $(x^4 + x^2 + x + 1) \otimes (x^6 + x^4 + x + 1) = x^4(x^6 + x^4 + x + 1) + x^2(x^6 + x^4 + x + 1) + x(x^6 + x^4 + x + 1) + (x^6 + x^4 + x + 1) = x^{10} + x^8 + x^5 + x^4 + x^8 + x^6 + x^3 + x^2 + x^7 + x^5 + x^2 + x + x^6 + x^4 + x + 1 = x^{10} + x^7 + x^3 + 1$

$x^{10} + x^7 + x^3 + 1$	$x^7 + x^3 + x^2 + 1$
$x^{10} + x^6 + x^5 + x^3$	$x^3 + 1$
$x^7 + x^6 + x^5 + 1$	
$x^7 + x^3 + x^2 + 1$	
$x^6 + x^5 + x^3 + x^2$	

$$(x^4 + x^2 + x + 1) \otimes (x^6 + x^4 + x + 1) = (x^6 + x^5 + x^3 + x^2) mod (x^7 + x^3 + x^2 + 1)$$

4 Для каждого из слов найти полиномы, которые представляют эти слова

1 111111→8 бит

$$1 \cdot x^6 + 1 \cdot x^5 + 1 \cdot x^4 + 1 \cdot x^3 + 1 \cdot x^2 + 1 \cdot x^1 + 1 \cdot x^0 = x^6 + x^5 + x^4 + x^3 + x^2 + 1$$

5 Найти сумму и произведение двух полиномов по модулю, найти мультипликативную инверсию для одного из чисел в поле Галуа

1) 43h = 1000011$\rightarrow x^6 + x + 1$
2) 06h = 110$\rightarrow x^2 + x$
3) $x^5 + x^3 + x^2 + 1$

Суммадвухполиномов:

1) $x^6 + x^1 + 1$
2) $x^2 + x^1$

$$(1 \cdot x^6 + +0 \cdot x^5 + 0 \cdot x^4 + 0 \cdot x^3 + 0 \cdot x^2 + 1 \cdot x^1 + 1 \cdot x^0) +$$
$$+ (0 \cdot x^6 + 0 \cdot x^5 + 0 \cdot x^4 + 0 \cdot x^3 + 1 \cdot x^2 + 1 \cdot x^1 + 0 \cdot x^0) = x^6 + x + 1$$

Ответ: $x^6 + x^2 + 1$

Произведение двух полиномов:

$$(x^6 + x^1 + 1) \cdot (x^2 + x) =$$
$$x^8 + x^7 + x^3 + x^2 + x^2 + x^1 + =$$
$$x^8 + x^7 + x^8 + x^4 + x^3 + x^2 + x$$

$x^8 + x^7 + x^3 + x^1$	$x^5 + x^3 + x^2 + 1$
$x^8 + x^6 + x^5 + x^3$	$x^3 + x^2 + x$
$x^7 + x^6 + x^5 + x^1$	
$x^7 + x^5 + x^4 + x^2$	
$x^6 + x^4 + x^2 + x^1$	
$x^6 + x^4 + x^3 + x^1$	
$x^3 + x^2$	

Мультипликативная инверсия:

$$(x^2 + x^1)^{-1} \mathrm{mod}\ (x^5 + x^3 + x^2 + 1)$$

I	a_j	y_j	q_j
0	$x^5 + x^3 + x^2 + 1$	0	-
1	$x^2 + x^1$	1	$x^3 + x^2$
2	$x^2 + 1$	$0\text{-}1(x^3 + x^{2)} = x^3 + x^2$	1
3	$x + 1$	$1\text{-}(x^3 + x^2) = x^3 + x^2 + 1$	x

4	$x + 1$	$x^3 + x^2 - (x^3 + x^2+1)x=$ $x^4 + x^2 + x$	1
5	0		

$q_1 = (x^5 + x^3 + x^2 + 1) / (x^2 + x^1) = x^3 + x^2$
$a_2 = (x^2 + x)/(x^2 + 1) = 1$
$q_3 = (x^2 + 1)(x + 1) = x$
$a_4 = (x + 1)/(x + 1) = 1$

Проверка:

$(x^4 + x^2 + x) \cdot x^2 + x^1 = x^6 + x^5 + x^4 + x^2$

$x^6 + x^5 + x^4 + x^2$ $x^6 + x^4 + x^3 + x$	$x^5 + x^3 + x^2 + 1$
$x^5 + x^3 + x^2 + x$ $x^5 + x^3 + x^2 + 1$	X+1
X+1	

Ответ: x+1

6 Для каждого из слов найти полиномы, которые представляют эти слова

1 0 1 0 1 0 1

$1 \cdot x^6 + 0 \cdot x^5 + 1 \cdot x^4 + 0 \cdot x^3 + 1 \cdot x^2 + 0 \cdot x^1 + 1 \cdot x^0 = x^6 + x^4 + x^2 + 1$

7 Найти сумму и произведение двух полиномов по модулю, найти мультипликативную инверсию для одного из чисел в поле Галуа

4) F3h = 243 = 1 1 1 1 0 0 1 1
5) 16h = 22 = 1 0 1 1 0
6) $x^5 + x^3 + x^2 + 1$

Суммадвухполиномов:

$$x^7 + x^6 + x^5 + x^4 + x + 1$$
$$x^4 + x^2 + x$$
$$(1 \cdot x^7 + 1 \cdot x^6 + 1 \cdot x^5 + 1 \cdot x^4 + 0 \cdot x^3 + 0 \cdot x^2 + 1 \cdot x^1 + 1 \cdot x^0) +$$
$$+ (1 \cdot x^4 + 0 \cdot x^3 + 1 \cdot x^2 + 1 \cdot x + 0 \cdot x^0) = x^7 + x^6 + x^5 + x^2 + x + 1$$

Ответ: $x^7 + x^6 + x^5 + x^2 + 1$

Произведение двух полиномов:

$$(x^7 + x^6 + x^5 + x^4 + x + 1) \cdot (x^4 + x^2 + x) =$$
$$x^{11} + x^9 + x^8 + x^{10} + x^8 + x^7 + x^9 + x^7 + x^6 + x^8 + x^6 + x^5 + x^5 + x^3 + x^4 + x^2 + x =$$
$$x^{11} + x^{10} + x^8 + x^4 + x^3 + x^2 + x$$

$x^{11} + x^{10} + x^8 + x^4 + x^3 + x^2 + x$	$x^5 + x^3 + x^2 + 1$
$x^{11} + x^9 + x^8 + x^6$	$x^6 + x^5 + x^4 + x^2 + x$
$x^{10} + x^9 + x^6 + x^4 + x^3 + x^2 + x$	
$x^{10} + x^8 + x^7 + x^5$	
$x^9 + x^8 + x^6 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x$	
$x^9 + x^7 + x^6 + x^4$	
$x^8 + x^5 + x^3 + x^2 + x$	
$x^8 + x^6 + x^5 + x^3$	
$x^6 + x^2 + x$	
$x^6 + x^4 + x^3 + x$	
$x^4 + x^3 + x^2$	

Ответ: $(x^7 + x^6 + x^5 + x^4 + x + 1) * (x^4 + x^2 + x) \bmod (x^5 + x^3 + x^2 + 1) =$
$=x^6 + x^5 + x^4 + x^2 + x$

Мультипликативная инверсия:

$$(x^4 + x^2 + x)^{-1} \bmod (x^5 + x^3 + x^2 + 1)$$

I	a_i	y_i	q_i
0	$x^5 + x^3 + x^2 + 1$	0	-
1	$x^4 + x^2 + x$	1	x
2	1	x	$x^4 + x^2 + x$
3	0		

$q_1 = (x^5 + x^3 + x^2 + 1) / (x^4 + x^2 + x) = x$
$a_2 = (x^5 + x^3 + x^2 + 1) - ((x^4 + x^2 + x) \cdot (x)) = 1$
$q_2 = (x^4 + x^2 + x) / 1 = x^4 + x^2 + x$
$a_2 = (x^4 + x^2 + x) - (1 \cdot (x^4 + x^2 + x)) = 0$

Проверка:
$(x^4 + x^2 + x) \cdot x = (x^5 + x^3 + x^2 + 1)$

$x^5 + x^3 + x^2$	$x^5 + x^3 + x^2 + 1$
$x^5 + x^3 + x^2 + 1$	1
1	

Ответ: x

8 Найти сумму и произведение двух полиномов по модулю, найти мультипликативную инверсию для одного из чисел в поле Галуа.

D3h 11010011_2 $P_1=x^7+x^6+x^4+x^1+x^0$

06h110_2 $P_2=x^2+x^1$

11010101_2 P=$x^7+x^6+x^4+x^2+1$

$P_1 \otimes P_2 = x^2(x^7+x^6+x^4+x^1+1)+x(x^7+x^6+x^4+x^1+1) =$

$= x^9+\cancel{x^8}+x^6+x^3+\cancel{x^2}+\cancel{x^8}+x^7+x^5+\cancel{x^2}+x^1=x^9+x^7+x^6++x^5+x^3+x$

$x^9+x^7+x^6+x^5+x^3+x$	$x^6+x^3+x^2+1$
$x^9+x^6+x^5+x^3$	
x^7+x	x^3+x
$x^7+x^4+x^3+x$	
$-x^4-x^3$	

Остаток: $-x^4-x^3$

Мультипликативная инверсия

i	a_i	y_i	q_i
0	$x^6+x^3+x^2+1$	0	—
1	$x^7+x^6+x^4+x+1$	1	0
2	$x^6+x^3+x^2+1$	0	x+1
3	x^2	1	x^4+x+1
4	1	x^4+x+1	x^2
5	0		

Проверка:

$(x^4+x+1)*(x^7+x^6+x^4+x+1) = x^{11}+\cancel{x^{10}}+\cancel{x^8}+\cancel{x^5}+\cancel{x^4}+\cancel{x^8}+\cancel{x^7}+\cancel{x^5}+x^2+\cancel{x}+\cancel{x^7}+x^6+\cancel{x^4}+\cancel{x}+1 = x^{11}+x^{10}+x^6+x^2+1$

$x^6+x^3+x^2+1$

$x^{11}+x^{10}+x^6+x^2+1$	$x^6+x^3+x^2+1$
$x^{11}+x^8+x^7+x^5$	
$x^{10}+x^8+x^7+x^6+x^5+x^2+1$	$x^5+x^4+x^2$
$x^{10}+x^7+x^6+x^4$	
$x^8+x^5+x^4+x^2+1$	
$x^8+x^5+x^4+x^2$	
1	

Остаток равен 1, следовательно, инверсия выполнена верно.

9Для каждого из слов найти полиномы, которые представляют эти слова:

010101

Решение: 010101 – 6 бит

$0X^5+1X^4+0X^3+1X^2+0X^1+1X^0=1X^4+1X^2+1=X^4+X^2+1$

Ответ: X^4+X^2+1

10Найти сумму и произведение двух полиномов по модулю, найти мультипликативную инверсию для одного из чисел в поле Галуа:

A8h

11h

$X^6+X^5+X^2+1$

Решение:

A8h – 10101000 – $1X^7+1X^5+1X^3$

11h – 1011 – $1X^3+1X^1+1X^0$

Сложение: 10101000+00001011=10100011

10100011 – $X^7+X^5+X^1+1$

Произведение по модулю: $P_1 \otimes P_2$

$(1X^7+0X^6+1X^5+0X^4+1X^3+0X^2+0X^1+0X^0)\otimes(1X^3+0X^2+1X^1+1X^0)=$

$(X^7+X^5+X^3)\otimes(X^3+X^1+X^0)=X^{10}+X^8+X^0+X^8+X^6+X^0+X^6+X^4+X^0=$

$=X^{10}+X^4+1$

$X^{10}+X^4+1$ | $X^6+X^5+X^2+1$

$X^{10}+X^9+X^6+X^4$ | $X^4+X^3+X^2+X+X$

X^9+X^6+1

$X^9+X^8+X^5+X^3$

$X^8+X^6+X^5+X^3+1$

$X^8+X^7+X^4+X^2$

$X^7+X^6+X^5+X^4+X^3+X^2+1$

$X^5+X^4+X^3+X$

$X^7+X^6+X^2+X+1$

$X^7+X^6+X^3+X$

X^3+X^2+1

Мультипликативная инверсия

i	a_i	y_i	q_i
0	$X^6+X^5+X^2+1$	0	–
1	X^3+X^1+1	1	$[a_0/a_1]$ $X^6+X^5+X^2+1$ | X^3+X^1+1 $X^6+X^4+X^3$ | $X^3+X^2+X^1$ $X^5+X^4+X^3+X^2+1$ $X^5+X^3+X^2$ X^4+1 $X^4+X^2+X^1$ X^2+X^1+1
2	X^2+X^1+1	$y_2=y_0-y_1\cdot q_1=$ $=0-1\cdot(X^3+X^2+X^1)=$ $=X^3+X^2+X^1$	$[a_1/a_2]$ X^3+X^1+1 | X^2+X^1+1 X^2+X^1+X | X^1 X^2+X^1
3	X^2+1	$y_3=y_1-y_2\cdot q_2=$ $=1-(X^3+X^2+X^1)\cdot X^1=$ $=1+(X^4+X^3+X^2)$	$[a_2/a_3]$ X^2+X^1+1 | X^2+1 X^2+1 | 1 X^1
4	X^1	$y_4=y_2-y_3\cdot q_3=$ $=X^4+X^1+1$	$[a_3/a_4]$ X^2+1 | X^1 X^2 | X^1 1
5	1	$y_5=y_3-y_4\cdot q_4=$ $=X^4+X^3+X^5+X^1+1$	$[a_4/a_5]$ X | 1 X | X 0
6	0		

Проверка: $(X^3+X^1+1)\otimes(X^5+X^4+X^3+X^1+1)=(X^8+X^7+X^6+X^4+X^3)+$
$+(X^6+X^5+X^4+X^2+X^4)+(X^5+X^4+X^3+X^4+1)=X^8+X^7+X^4+X^2+1$

$X^8+X^7+X^4+X^2+1$ \| $X^6+X^5+X^2+1$
$X^8+X^7+X^4+X^2$ \| X^2
1

Ответ: $X^4+X^3+X^5+X^1+1$

8.4Упражнения к практической работе

1.Для каждого из слов найти полиномы, которые представляют эти слова (варианты заданий 1 представлены в таблице 8.2):

Таблица 8. 2 – Выбор варианты задания 1

Вариант 1	Вариант 2	Вариант 3	Вариант 4
10010	010101	1111111	0101111
Вариант 5	Вариант 6	Вариант 7	Вариант 8
100001	101111	1110001	1001101
Вариант 9	Вариант 10	Вариант 11	Вариант 12
1110001	00011	1010101	001101
Вариант 13	Вариант 14	Вариант 15	Вариант 16
100011	100110	1110000	110000

2 Найти сумму и произведение двух полиномов по модулю, найти мультипликативную инверсию для одного из чисел в поле Галуа (варианты задания 2 приведены в таблице 8.3):

Таблица 8.3 – выбор варианта для задания 2

Вариант 1	Вариант 2	Вариант 3	Вариант 4
58h 32h X^4+x^3+1	A8h 11h $X^6+x^5+x^2+1$	43h 06h $X^5+x^3+x^2+1$	43h 06h $X^5+x^3+x^2+1$
Вариант 5	Вариант 6	Вариант 7	Вариант 8
03h 24h x^3+x^2+1	17h 53h $X^7+x^3+x^2+1$	43h A6h $X^7+x^3+x^2+1$	77h C8h $X^5+x^4+x^2+1$
Вариант 9	Вариант 10	Вариант 11	Вариант 12
C3h 06h $X^4+x^3+x^2+1$	D3h 06h $X^6+x^3+x^2+1$	F3h 16h $X^5+x^3+x^2+1$	A3h 16h $X^7+x^5+x^2+1$
Вариант 13	Вариант 14	Вариант 15	Вариант 16
43h A6h $X^5+x^3+x^2+1$	23h D6h $X^5+x^4+x^3+1$	33h C6h $X^7+x^3+x^2+1$	43h 06h $X^7+X^5+x^3+x^2+1$

8.4 Контрольные вопросы

1. Раскройте понятие Поля Галуа.
2. Раскройте основные операции в Поле Галуа (2).
3. Что представляет собой полином. Как представить двоичное число с помощью полинома.
4. Как найти сумму, произведение двух полиномов.
5. Как найти мультипликативную инверсию в полиномиальном виде.

Список использованных источников

1. Биркгоф, Г. Современная прикладная алгебра = ModernAppliedAlgebra : пер. с англ. / Г. Биркгоф, Т.К. Барти. – 2-е изд., стер. – СПб. : Лань, 2005. – 400 с.
2. Виноградов, И.М. Элементы высшей математики : учеб. для вузов / И.М. Виноградов. – М.: Высш. шк., 1999. – 511 с.
3. Введение в криптографию: учеб. / под ред. В.В. Ященко. – Спб.: Питер, 2001. – 348 с.
4. Василенко, О. Н. Теоретико-числовые алгоритмы в криптографии : монография / О. Н. Василенко. – М. : МЦНМО, 2003. – 328 с.
5. Домарев, В.В. Защита информации и безопасность компьютерных систем / В.В. Домарев. – Киев : Диа-Софт, 1999. – 480 с.
6. Жельников, В. Криптография от папируса до компьютера / В. Жельников. – М. : ABF, 1996. – 336с.
7. Зегжда, Д.П. Основы безопасности информационных систем: учеб. пособие / Д.П. Зегжда, А.М. Ивашко. – М. : Горячая линия – Телеком, 2000. – 452 с.
8. Логачев, О.А. Булевы функции в теории кодирования и криптологии / О.А. Логачев, А.А. Сальников, В.В. Ященко. – М. : МЦНМО, 2004. – 470 с.
9. Нечаев, В.И. Элементы криптографии. Основы теории защиты информации: учеб. пособие / В.И. Нечаев. – М. : Высш. шк., 1999. – 109 с.
10. Открыванкина, Т.М. Алгоритмы компьютерной алгебры: практикум/ Т.М. Отрыванкина; М-во образования и науки Рос. Федерации, Федер. агентство по образованию, Гос. образоват. учреждение высш. проф. образования "Оренбург.гос. ун-т", Каф. приклад. математики. - Оренбург : ГОУ ОГУ, 2007. – 26 с.
11. Проскурин, В.Г. Программно-аппаратные средства обеспечения информационной безопасности. Защита в операционных системах: учеб. пособие для вузов / Проскурин В.Г., Крутов С.В., Мацакевич И.В. – М.: Радио и связь, 2000. – 166 с.
12. Романец, Ю.В. Защита информации в компьютерных системах и сетях / Ю.В. Романец, П.А. Тимофеев, В.Ф. Шаньгин; под ред. В.Ф. Шаньгина. 2-е изд., перераб. и доп. – М. : Радио и связь, 2001. – 376 с.
13. Судоплатов, С.В. Элементы дискретной математики : учеб. для вузов / С.В. Судоплатов, Е.В. Овчинникова. – Новосибирск: НГТУ, 2002. – 280 с.
14. Хаггарти, Р. Дискретная математика для программистов: пер. с англ: учеб. пособие для вузов / Р. Хаггарти. – М.: Техносфера, 2005. – 320с.