ВОЕННО-КОСМИЧЕСКАЯ АКАДЕМИЯ
имени А.Ф. Можайского

К.Ю. Цветков, В.М. Коровин

РЕШЕНИЕ ЗАДАЧ ПО ТЕОРИИ ИНФОРМАЦИИ И КОДИРОВАНИЯ

Учебное пособие

Санкт-Петербург
2014

Рецензенты:
доктор технических наук, профессор **М.А. Еремеев**;
кандидат технических наук **А.В. Галанкин**

Цветков К.Ю.

Решение задач по теории информации и кодирования: учеб. пособие / К. Ю. Цветков, В.М. Коровин. – СПб.: ВКА имени А. Ф. Можайского, 2014. – 63 с.

Учебное пособие адресовано обучающимся по специальности «Сети и системы связи космических комплексов». Также учебное пособие может быть использовано специалистами в области проектирования и организации вычислительных и телекоммуникационных систем.

Подписано к печ. 11.12.2013 | Формат печатного листа 445×300/8
Гарнитура Times New Roman | Авт. л. 3,75
Уч.-печ. л. 8,00 | Заказ 2696 | Бесплатно

Типография ВКА имени А.Ф. Можайского

ОГЛАВЛЕНИЕ

Предисловие

Учебное пособие написано по опыту преподавания авторами дисциплин «Информатика», «Теория электрической связи» и «Терия информации и кодирования» в Военно-космической академии имени А.Ф. Можайского и адресовано обучающимся по специальности «Сети и системы связи космических комплексов». Также учебное пособие может быть использовано специалистами в области телекоммуникационных систем и связи.

При написании пособия авторы придерживались принципа необходимости привития обучающимся практических навыков при решении задач по дисциплине «Терия информации и кодирования». Авторы показали в учебном пособии различные способы решения однотипных задач, подробно описали решение задач, которые обычно вызывают трудности у обучаемых. Пособие ориентировано на читателя, который стремится более глубоко изучить вопросы дисциплины и не довольствуется только тем материалом, который предлагается на лекциях.

Авторы выражают благодарность рецензентам за кропотливый труд по поиску ошибок и неточностей, а также ценные замечания, которые помогли сделать материал пособия лучше и доступнее.

1 ЭЛЕМЕНТЫ ТЕОРИИ ЧИСЕЛ

Теория чисел занимается изучением свойств целых чисел. Для их обозначения будут использоваться буквы a, b, c... Рассматриваются четыре арифметических операции: сложение, вычитание, умножение и деление. В результате первых трех операций также получаются целые числа. Операция деления может выполняться как нацело, так и с остатком. В первом случае, когда $a = b \cdot q$, делимое a называется кратным числа b, b называется делителем, q – частным. При этом для отражения того факта, что b есть делитель a, используется обозначение $b|a$ (b делит a).

При делении с остатком используется выражение $a = bq+r$, $0 \le r < b$, в котором q называется неполным частным, а r – остатком.

Определение. Всякое целое, делящее одновременно целые $a, b,...,l$ называется их о б щ и м д е л и т е л е м .

Определение. Н а и б о л ь ш и й о б щ и й д е л и т е л ь – это наибольший из всех общих делителей чисел $a, b,...,l$, который обозначается

$$\text{НОД}(a, b,...,l) = (a, b,...,l).$$

Определение. Если $(a, b,...,l) = 1$, то числа $a, b,...,l$ называются в з а и м н о п р о с т ы м и .

1.1 Алгоритм Евклида

1. Задаются два числа a и b.
2. Последовательно находится ряд равенств:

$$\left.\begin{aligned} a &= bq_1 + r_2, & 0 < r_2 < b,\\ b &= r_2q_2 + r_3, & 0 < r_3 < r_2,\\ r_2 &= r_3q_3 + r_4, & 0 < r_4 < r_3,\\ &\cdots & \cdots\\ r_{n-2} &= r_{n-1}q_{n-1} + r_n, & 0 < r_n < r_{n-1},\\ r_{n-1} &= r_nq_n. \end{aligned}\right\}$$

3. Алгоритм заканчивается, когда $r_{n+1} = 0$:

$$(a, b) = r_n.$$

Определение. Н а и м е н ь ш и м о б щ и м к р а т н ы м (НОК) совокупности чисел называется наименьшее положительное число, кратное всем данным числам.

Для двух чисел a и b общее кратное и наименьшее общее кратное определяется в соответствии с выражением

$$M = \frac{ab}{d}t,$$

где $d = (a, b)$ – наибольший общий делитель; t – целое.

1.2 Функция Эйлера

Определение. Функция Эйлера $\varphi(a)$ определяется для всех целых положительных a и представляет собою число чисел ряда

$$0, 1, ..., a-1,$$

взаимно простых с a.

1.3 Сравнения и их свойства

Каждому целому числу a отвечает определенный остаток r при делении его на m. Если двум целым a и b отвечает один и тот же остаток r, то они называются равноостаточными по модулю m или сравнимыми по модулю m.

Сравнимость чисел a и b по модулю m записывается следующим образом:

$$a \equiv b \bmod m.$$

Сравнимость равносильна возможности представить число a в виде $a = b+mt$, где t – целое.

1.4 Свойства сравнений, аналогичные свойствам равенств

1. Два числа, сравнимые с третьим, сравнимы между собой:

$$a \equiv b \bmod m \text{ и } c \equiv b \bmod m \Rightarrow a \equiv c \bmod m.$$

2. Сравнения можно почленно складывать:

$$a_1 \equiv b_1 \bmod m,\ a_2 \equiv b_2 \bmod m \Rightarrow a_1+a_2 \equiv (b_1+b_2) \bmod m.$$

3. Слагаемое, стоящее в какой-либо части сравнения, можно переносить в другую часть, переменив знак на обратный.

4. К каждой части сравнения можно прибавить любое число, кратное модулю.

5. Сравнения можно почленно перемножать.

6. Обе части сравнения можно возвести в одну и ту же степень.

7. Обе части сравнения можно умножить на одно и то же целое.

8. Обе части сравнения можно разделить на их общий делитель, если последний взаимно прост с модулем.

В приведенных свойствах сравнений модуль остается неизменным. Рассмотрим свойства сравнений, в которых модуль изменяется.

1.5 Свойства сравнений с изменяемым модулем

1. Обе части сравнения и модуль можно умножить на одно и то же целое, например:

$$9 \equiv 5 \bmod 4: 9\cdot 6 = 54 \equiv 6 \bmod 24,\ 5\cdot 6 \equiv 6 \bmod 24,\ 6 = 6.$$

2. Обе части сравнения и модуль можно разделить на любой их общий делитель, например:

$$40 \equiv 8 \bmod 16:\ \ 40:8 \equiv 1 \bmod 2,\ \ 8:8 \equiv 1 \bmod 2,\ 1 = 1.$$

3. Если сравнение $a \equiv b$ имеет место по нескольким модулям, то оно имеет место и по модулю, равному наименьшему общему кратному этих модулей, например:

$$34 \equiv 4 \bmod 5,\ 34 \equiv 4 \bmod 6,\ 34 \equiv 4 \bmod 15.$$

НОК модулей 5, 6 и 15 равен $[5,6,15] = 30$, $34 \equiv 4 \bmod 30$.

4. Если сравнение имеет место по модулю m, то оно имеет место и по модулю d, равному любому делителю числа m, например:

$$11 \equiv 5 \bmod 6: d = 3,\ 11 \equiv 2 \bmod 3,\ 5 \equiv 2 \bmod 3,\ 2 = 2.$$

5. Если одна часть сравнения и модуль делятся на какое-либо число, то и другая часть сравнения должна делиться на то же число, например:

$$24 \equiv 6 \bmod 9:\ 24:3 = 8,\ 9:3 = 3, \text{ следовательно, } 6:3 = 2.$$

6. Если $a \equiv b \bmod m$, то $(a, m) = (b, m)$, например:

$$24 \equiv 6 \bmod 9: (24,9) = 3, (6,9) = 3.$$

1.6 Полная и приведенная системы вычетов

Числа, сравнимые по модулю m, образуют класс чисел по модулю m. Всем числам класса отвечает один и тот же остаток r. Так как r может принимать значения от нуля до m–1, то имеется m различных классов чисел по модулю m.

Определение. Вычетом по модулю m называется любое число класса чисел, сравнимых по модулю m, по отношению ко всем числам этого же класса. Вычет, равный самому остатку r, называется наименьшим неотрицательным вычетом.

Определение. Полной системой вычетов называется совокупность вычетов, взятых по одному из каждого класса. Чаще всего в качестве полной системы вычетов употребляют наименьшие неотрицательные вычеты 0, 1,..., m–1.

Определение. Приведенной системой вычетов по модулю m называется совокупность вычетов, взаимно простых с модулем.

Приведенную систему вычетов можно выделить из системы наименьших неотрицательных вычетов. Число элементов приведенной системы вычетов по модулю m определяется функцией Эйлера $\varphi(m)$.

Теорема Эйлера. При $m > 1$ и $(a,m) = 1$ выполняется сравнение

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

Например, при $m = 9$, $a = 2$ значение функции Эйлера $\varphi(m) = 6$. Тогда $2^6 = 64 \equiv 1 \bmod 9$.

1.7 Сравнения с одним неизвестным

Аналогично уравнениям с одним неизвестным можно рассматривать сравнения с одним неизвестным следующего вида:

$$f(x) \equiv 0 \bmod m;\ f(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_i x + a_0.$$

Если a_n не делится на m, то n называется степенью сравнения.

Решить сравнение – значит найти все значения x, ему удовлетворяющие. Два сравнения, которым удовлетворяют одни и те же значения x, называются равносильными.

Если сравнению удовлетворяет какое-либо $x = x_1$, то ему будут удовлетворять и все числа, сравнимые с x_1 по модулю m: $x = x_1 \bmod m$. Весь этот класс чисел считается за одно решение. Таким образом, сравнение будет иметь столько решений, сколько вычетов полной системы ему удовлетворяют.

Рассмотрим сравнения первой степени, которые за счет переноса свободного члена в правую часть можно привести к виду

$$ax \equiv b \bmod m.$$

Определим число решений сравнения при условии $(a,m) = 1$. В этом случае при пробегании x полной системы вычетов, форма ax также пробегает полную систему вычетов. Следовательно, ax будет сравнимо с b только при одном значении x. Таким образом, при $(a,m) = 1$ сравнение имеет только одно решение.

Пусть теперь $(a,m) = d > 1$. Тогда, чтобы сравнение имело решения, необходимо, чтобы b делилось на d, иначе сравнение невозможно ни при каком целом x. Полагая $a = a_1d$, $b = b_1d$, $m = m_1d$, сравнение можно привести к виду

$$a_1x \equiv b_1 \bmod m_1,\ (a_1, m_1) = 1.$$

Данное сравнение имеет одно решение по модулю m_1. Пусть x_1 – наименьший неотрицательный вычет этого решения по модулю m_1, тогда все числа, образующие это решение, найдутся в виде

$$x = x_1 \bmod m_1.$$

По модулю же m числа x образуют не одно решение, а больше, именно d решений, которые лежат в ряду от нуля до $m–1$.

Таким образом, при $(a,m) = d$ исходное сравнение имеет d решений: x_1, x_1+m_1, $x_1+2m_1,\ldots, x_1+(d–1)m_1$.

Одним из способов решения сравнений первой степени вида является способ, основанный на использовании алгоритма Евклида нахождения наибольшего общего делителя.

Решение сравнения первой степени для $(a,m) = 1$ определяется выражением

$$x \equiv (–1)^{n–1}P_{n–1}b \bmod m,$$

где n – число неполных делителей при выполнении алгоритма Евклида для отношения m/a; $P_{n–1}$ – $(n–1)$-е значение текущего вспомогательного параметра, определяемого через неполные частные q_i. Данный вспомогательный параметр определяется следующей формулой при начальных условиях $P_{–1} = 0$, $P_0 = 1$:

$$P_i = q_iP_{i–1} + P_{i–2}.$$

1.8 Алгоритм решения сравнения первой степени

Рассмотрим сравнение первой степени:

$$ax \equiv b \bmod m.$$

1. Определить НОД: если $(a, m) = 1$, то перейти к п. 4; если $(a, m) = d$, то перейти к п. 2.

2. Проверить, делится ли b на d: если $d \mid b$, то перейти к п. 3, иначе сделать вывод, что сравнение не имеет решений.

3. Разделить левую, правую часть сравнения и модуль на число d:

$$a_1x \equiv b_1 \bmod m_1,\ (a_1, m_1) = 1.$$

4. Определить параметр $P_{n–1}$, выполнив алгоритм Евклида для отношения m/a или m_1/a_1:

а) определить неполные частные q_i, $i = \overline{1, n}$;

б) определить $P_i = q_iP_{i–1}+P_{i–2}$ для $i = n–1$, если $P_{–1} = 0$, $P_0 = 1$.

5. Определить решение сравнения

$$x_1 \equiv (-1)^{n-1} P_{n-1} b \bmod m.$$

6. Если $(a, m) = 1$, то завершить алгоритм с данным единственным решением x_1.

7. Если $(a, m) = d$, то определить остальные решения сравнения: x_1+m_1, x_1+2m_1, ..., $x_1+(d-1)m_1$.

1.9 Первообразные корни и индексы

Для любого целого a, взаимно простого с m, т.е. при условии, что $(a, m) = 1$, при возведении данного a в последовательные степени всегда найдется такое минимальное положительное число ε, для которого выполняется сравнение

$$a^{\varepsilon} \equiv 1 \bmod m.$$

Минимальное положительное ε, для которого выполняется данное сравнение, называется показателем, которому a принадлежит по модулю m.

В некоторых случаях число ε называется периодом элемента a, что отражает периодическую повторяемость элементов при возведении a в последовательные степени.

При дальнейшем возведении элементов a_i в последовательные степени наблюдается их периодическая повторяемость по модулю m.

Утверждение. Если a по модулю m принадлежит показателю ε, то числа $1 = a^0, a^1, ..., a^{\varepsilon-1}$ по модулю m несравнимы.

Утверждение. Показатели, которым числа принадлежат по модулю m, суть делители $\varphi(m)$.

Определение. Числа, принадлежащие показателю $\varphi(m)$, называются первообразными корнями по модулю m.

Первообразные корни будем обозначать буквой α.

Все вышеизложенное справедливо и для приведенных систем вычетов по составному модулю.

Таким образом, последовательные степени чисел, являющихся первообразными корнями, пробегают все элементы как полной, так и приведенной системы вычетов по модулю m.

Для чисел a, взаимно простых с m, вводится понятие об индексе, представляющее аналогию понятия о логарифме; при этом первообразный корень α играет роль, аналогичную роли основания логарифма.

Определение. Индексом числа a по модулю m при основании α называется наименьшее число $I \geq 0$, для которого выполняется равенство

$$a \equiv \alpha^I \bmod m.$$

Индекс числа a обозначается $I = \mathrm{ind}_{\alpha} a$ или $I = \mathrm{ind}\, a$.

Для каждого простого p составляются две таблицы; первая – для нахождения индекса по числу, вторая – для нахождения числа по индексу. Таблицы содержат наименьшие неотрицательные вычеты чисел (приведенная система) и их наименьших индексов (полная система) соответственно по модулям p и $c = \varphi(p) = p-1$.

1.10 Задачи

Задача 1.1. Разложить числа на множители:

а) 90; б) 336; в) 414.

Задача 1.2. Разложить числа на множители. В ответе указать сумму простых множителей, больших 1:

а) 2394; б) 3234; в) 2184; г) 2574.

Задача 1.3. Определить общие делители чисел:

а) 90 и 48; б) 78 и 36; в) 169 и 52.

Задача 1.4. Определить наибольший общий делитель чисел:

а) (60, 45, 75); б) (48, 32); в) (64, 27).

Задача 1.5. Найти наибольший общий делитель:

а) (60, 36); б) (56, 42); в) (68, 24); г) (70, 54); д) (30, 80); е) (54, 18); ж) (72, 44).

Задача 1.6. Найти наибольший общий делитель с помощью алгоритма Евклида:

а) (553, 623); б) (424, 156); в) (336, 292); г) (671, 1067); д) (468, 747); е) (354, 432); ж) (525, 231); з) (636, 153).

Задача 1.7. Найти наибольший общий делитель с помощью алгоритма Евклида:

а) (2184, 2574); б) (2394, 3234); в) (2394, 2184); г) (2394, 2574); д) (3234, 2184); е) (3234, 2574); ж) (2550, 3808); з) (2640, 1365).

Задача 1.8. Представить каноническое разложение чисел на множители. Определить число делителей чисел:

а) 726; б) 144; в) 108; г) 72; д) 528; е) 132300; ж) 588000; з) 56700; и) 6480; к) 330750; л) 6860.

Задача 1.9. Найти наименьшее общее кратное:

а) [60, 36]; б) [70, 54]; в) [56, 42]; г) [68, 24]; д) [30, 80]; е) [54, 18]; ж) [72, 44].

Задача 1.10. Определить общие кратные и НОК для чисел:

а) [6, 8]; б) [12, 15]; в) [4, 9]; г) [15, 18]; д) [21, 35]; е) [42, 39].

Задача 1.11. Определить функцию Эйлера для чисел:

а) $\varphi(132300)$; б) $\varphi(588000)$; в) $\varphi(1620)$; г) $\varphi(999)$; д) $\varphi(1044)$; е) $\varphi(94)$; ж) $\varphi(39)$; з) $\varphi(72)$; и) $\varphi(2310)$.

Задача 1.12. Вычислить сравнения по модулю $m = 5$:

а) 17 mod 5; б) –11 mod 5; в) 136 mod 5; г) 355 mod 5.

Задача 1.13. Вычислить сравнения по модулю:

а) 25 mod 8; б) 5 mod 2; в) 10 mod 7; г) –15 mod 7; д) –10 mod 2; е) –9 mod 4.

Задача 1.14. Вычислить сравнения по модулю:

а) 5 mod 2; б) 10 mod 5; в) 7 mod 10; г) 14 mod 3; д) –6 mod 5; е) –20 mod 13; ж) 11 mod 7; з) 19 mod 13; и) 10356 mod 29.

Задача 1.15. Верны ли сравнения?

а) $15 \equiv 5 \bmod 3$; б) $28 \equiv 3 \bmod 5$; в) $23 \equiv 4 \bmod 4$; г) $16 \equiv 2 \bmod 7$; д) $3 \equiv 2 \bmod 2$; е) $12 \equiv 3 \bmod 3$.

Задача 1.16. Определить элементы приведенной системы вычетов и значение функции Эйлера:

а) m = 42; б) m = 39; в) m = 37.

Задача 1.17. Решить сравнения:

а) $x^4+x+2 \equiv 0 \bmod 5$;

б) $32x \equiv 102 \bmod 123$;

в) $111x \equiv 75 \bmod 321$;

г) $81x \equiv 34 \bmod 95$;

д) $124x \equiv 88 \bmod 144$;

е) $351x \equiv 99 \bmod 198$.

Задача 1.18. Решить сравнения:

а) $134x \equiv 92 \bmod 152$;

б) $128x \equiv 34 \bmod 146$;

в) $122x \equiv 96 \bmod 134$;

г) $126x \equiv 38 \bmod 142$;

д) $130x \equiv 58 \bmod 144$;

е) $132x \equiv 82 \bmod 142$;

ж) $152x \equiv 29 \bmod 211$;

з) $579x \equiv 273 \bmod 462$.

Задача 1.19. Для системы вычетов по модулю $m = 5$ определить показатели, которым принадлежат элементы:

а) $a_1 = 1$; б) $a_2 = 2$; в) $a_3 = 3$; г) $a_4 = 4$.

Задача 1.20. Для системы вычетов по модулю $m = 7$ определить показатели, которым принадлежат элементы:

$a_1 = 1$, $a_2 = 2$, ... $a_6 = 6$.

Задача 1.21. Определить показатели, которым принадлежат элементы приведенной системы вычетов по модулю $m = 9$.

Задача 1.22. Определить показатели, которым принадлежат элементы приведенной системы вычетов по модулю $m = 10$.

Задача 1.23. Для системы вычетов по модулю m определить показатели, которым принадлежат элементы a_1, a_2.

а) m = 9, $a_1 = 4$, $a_2 = 2$; б) m = 7, $a_1 = 2$, $a_2 = 3$.

Задача 1.24. Определить первообразные корни по модулю m:

а) m = 3; б) m = 4.

Задача 1.25. Построить таблицы индексов для модуля $p = 13$ для наименьшего первообразного корня.

Задача 1.26. Построить таблицы индексов по модулю $p = 13$ для наибольшего первообразного корня.

Задача 1.27. Определить индексы элементов приведенной системы вычетов по модулю $m = 9$ для первообразного корня $\alpha = 5$.

Задача 1.28. Определить индексы элементов приведенных систем вычетов по модулям $m_1 = 10$ и $m_2 = 12$ для наибольших первообразных корней.

1.11 Решения

Решение к задаче 1.1.

а)	90	2	б)	336	2	в)	414	2
	45	3		168	2		207	3
	15	3		84	2		69	3
	5	5		42	2		23	23
				21	3			
				7	7			

Ответ: а) $90 = 2\cdot3^2\cdot5$; б) $336 = 2^4\cdot3\cdot7$; в) $414 = 2\cdot3^2\cdot23$.

Решение к задаче 1.2.

а) $2394 = 2\cdot3^2\cdot7\cdot19$, $s = 2 + 3 + 7 + 19 = 31$;

б) $3234 = 2\cdot3\cdot7^2\cdot11$, $s = 2 + 3 + 7 + 11 = 23$;

в) $2184 = 2^3\cdot3\cdot7\cdot13$, $s = 2 + 3 + 7 + 13 = 25$;

г) $2574 = 2\cdot3^2\cdot11\cdot13$, $s = 2 + 3 + 11 + 13 = 29$.

Решение к задаче 1.3.

а) 90 и 48.

Раскладываем числа на множители:

$90 = 2\cdot3\cdot3\cdot5$, $48 = 2\cdot2\cdot2\cdot2\cdot3$.

Общие делители: $q_1 = 2$, $q_2 = 3$, $q_3 = 6$, так как общими в разложениях являются числа 2 и 3.

Ответ: $q_1 = 2$, $q_2 = 3$, $q_3 = 6$.

б) 78 и 36.

Раскладываем числа на множители:

$78 = 2\cdot3\cdot13$, $36 = 2\cdot2\cdot3\ 3$.

Общие делители: $q_1 = 2$, $q_2 = 3$, $q_3 = 6$, так как общими в разложениях являются числа 2 и 3.

Ответ: $q_1 = 2$, $q_2 = 3$, $q_3 = 6$.

в) 169 и 52.

Раскладываем числа на множители:

$169 = 13\ 13$, $52 = 2\cdot2\cdot13$.

Общие делители: $q_1 = 13$, так как общим в разложениях является число 13.

Ответ: $q_1 = 13$.

Решение к задаче 1.4.

а) (60, 45, 75);

Раскладываем числа на множители

$60 = 2\cdot2\cdot\underline{3\cdot5}$, $45 = 3\cdot\underline{3\cdot5}$, $75 = \underline{3\cdot5}\cdot5$,

тогда (60, 45, 75) = 15, т.е. произведению совпадающих множителей.

Ответ: (60, 45, 75) = 15.

б) $48 = \underline{2\cdot2\cdot2\cdot2}\cdot3$, $32 = \underline{2\cdot2\cdot2\cdot2}\cdot2$, тогда $(48, 32) = 2^4 = 16$.

Ответ: (48, 32) = 16.

в) $64 = 2^6$, $27 = 3^3$, тогда (64, 27) = 1, т.е. числа 64 и 27 взаимно простые.

Ответ: (64, 27) = 1.

Решение к задаче 1.5.

а) 60 = 2·2·3·5, 36 = 2·2·3·3. Ответ: (60,36) = 12;

б) 56 = 2·2·2·7, 42 = 2·3·7. Ответ: (56,42) = 14;

в) 68 = 2·2·17, 24 = 2·2·2·3. Ответ: (68,24) = 4;

г) 70 = 2·5·7, 54 = 2·3·3·3. Ответ: (70,54) = 2;

д) 30 = 2·3·5, 80 = 2·2·2·2·5. Ответ: (30,80) = 10;

е) 54 = 2·3·3·3, 18 = 2·3·3. Ответ: (54, 18) = 18;

ж) 72 = 2·2·2·3·3, 44 = 2·2·11. Ответ: (72,44) = 4.

Решение к задаче 1.6.

а) (553,623)

_623	553	
553	1	
_553	70	r_1
490	7	
_70	63	r_2
63	1	
_63	7	r_3
63	9	
0		r_4

Результатом является последний положительный остаток $r_3 = 7$.

Ответ: (553,623) = 7.

б) (424,156)

_424	156	
312	2	
_156	112	r_1
112	1	
_112	44	r_2
88	2	
_44	24	r_3
24	1	
_24	20	r_4
20	1	
_20	4	r_5
20	5	
0		r_6

Результатом является последний положительный остаток $r_5 = 4$.

Ответ: (424,156) = 4.

в) (336,292)

_336	292	
292		
_292	44	r_1
264	6	
_44	28	r_2
28	1	
_28	16	r_3
16	1	
12		r_4

```
  _16 | 12
   12 | 1
_12   |  4   r5
 12   | 3
  0   r6
```

Результатом является последний положительный остаток $r_5 = 4$.

Ответ: (336,292) = 4.

г) (671,1067)

```
_1067 | 671
  671 | 1
_671  | 396   r1
  396 | 1
_396  | 275   r2
  275 | 1
_275  | 121   r3
  242 | 1
_121  | 33    r4
   99 | 3
 _33  | 22    r5
   22 | 1
 _22  | 11    r6
  22  | 2
   0  r7
```

Результатом является последний положительный остаток $r_6 = 11$.

Ответ: (671,1067) = 11.

д) (468,747)

```
_747 | 468
 468 | 1
_468 | 279   r1
 279 | 1
_279 | 189   r2
 189 | 1
_189 |  90   r3
 180 | 2
 _90 |  9    r4
  90 | 10
   0  r5
```

Результатом является последний положительный остаток $r_4 = 9$.

Ответ: (468,747) = 9.

е) (354,432)

```
_432 | 354
 354 | 1
_354 |  78   r1
 312 | 4
 _78 |  42   r2
  42 | 1
  36  r3
```

```
  _42 | 36
   36 | 1
_36   |  6    r4
 36   | 6
 ---  |
  0   | r5
```

Результатом является последний положительный остаток $r_4 = 6$.

Ответ: (354,432) = 6.

ж) (525, 231)

На основе процедуры последовательных делений (слева) получаем ряд равенств:

525 = 231·2+63, $r_1 = 63$;

231 = 63·3+42, $r_2 = 42$;

63 = 42·1+21, $r_3 = 21$;

42 = 21·2 $r_4 = 0$.

Последний положительный остаток $r_3 = 21$. Значит, (525, 231) = 21.

Ответ: (525, 231) = 21.

з) (636, 153)

```
          _636 | 153
           612 | 4
     _153      |  24    r1
      144      | 6
  _24          |  9     r2
   18          | 2
_9             |  6     r3
 6             | 1
_6             |  3     r4
 6             | 2
 ---           |
 0             | r5
```

Последний положительный остаток $r_4 = 3$.

Ответ: (636, 153) = 3.

Решение к задаче 1.7.

а) (2184, 2574) = 78, так как $2184 = 2^3 \cdot 3 \cdot 7 \cdot 13$; $2574 = 2 \cdot 3^2 \cdot 11 \cdot 13$;

б) (2394, 3234) = 42, так как $2394 = 2 \cdot 3^2 \cdot 7 \cdot 19$, $3234 = 2 \cdot 3 \cdot 7^2 \cdot 11$;

в) (2394, 2184) = 42, так как $2394 = 2 \cdot 3^2 \cdot 7 \cdot 19$, $2184 = 2^3\ 3\ 7\ 13$;

г) (2394, 2574) = 18, так как $2394 = 2 \cdot 3^2 \cdot 7 \cdot 19$, $2574 = 2\ 3^2\ 143$;

д) (3234, 2184) = 42, так как $3234 = 2\ 3\ 7^2\ 11$, $2184 = 2^3\ 3\ 7\ 13$;

е) (3234, 2574) = 6, так как $3234 = 2\ 3\ 7^2\ 11$, $2574 = 2\ 3^2\ 143$;

ж) (2550, 3808)=34, так как $2550 = 2\ 3\ 5^2\ 17$, $3808 = 2^5\ 7\ 17$;

з) (2640, 1365)=15, так как $2640 = 2^4\ 3\ 5\ 11$, $1365 = 3\ 5\ 7\ 13$.

Решение к задаче 1.8.

а) $726 = 2 \cdot 3 \cdot 11^2$, $N_d = (1+1)(1+1)(2+1) = 12$;

б) $144 = 2^4 \cdot 3^2$, $N_d = (4+1)(2+1) = 15$;

в) $108 = 2^2 \cdot 3^3$, $N_d = (2+1)(3+1) = 12$;

г) $72 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 = 2^3 \cdot 3^2$, $N_d = (3+1)(2+1) = 12$;

д) $528 = 2^4 \cdot 3 \cdot 11$, $N_d = (4+1)(1+1)(1+1) = 20$.

е) $132300 = 2^2 \cdot 3^3 \cdot 5^2 \cdot 7^2$, $N_d = (2+1)(3+1)(2+1)(2+1) = 108$

ж) $588000 = 2^5 \cdot 3 \cdot 5^3 \cdot 7^2$, $N_d = (5+1)(1+1)(3+1)(2+1)=144$;

з) $56700 = 2^2 \cdot 3^4 \cdot 5^2 \cdot 7^1$, $N_d = (2+1)(4+1)(2+1)(1+1)=90$;

и) $6480 = 2^4 \cdot 3^4 \cdot 5^1$, $N_d = (4+1)(4+1)(1+1)=50$;

к) $330750 = 2^1 \cdot 3^3 \cdot 5^3 \cdot 7^2$, $N_d = (1+1)(3+1)(3+1)(2+1)=96$;

л) $6860 = 2^2 \cdot 5^1 \cdot 7^3$, $N_d = (2+1)(1+1)(3+1)=24$.

Решение к задаче 1.9.

а) m = [60,36] = 60·36/(60,36) = 2160/12 = 180;

б) m = [70,54] = 70·54/(70,54) = 3780/2 = 1890;

в) m = [56,42] = 56·42/(56,42) = 2352/14 = 168;

г) m = [68,24] = 68·24/(68,24) = 1632/4 = 408;

д) m = [30,80] = 30·80/(30,80) = 2400/10 = 240:

е) m = [54,18] = 54·18/(54,18) = 972/18 = 54;

ж) m = [72,44] = 72·44/(72,44) = 3168/4 = 792.

Решение к задаче 1.10.

а) $m_1 = [6, 8] = 6 \cdot 8/(6, 8) = 48/2 = 24$; общие кратные: $M_1 = m_1 t = \{24, 48, 72,...\}$, $t \in Z$.

б) $m_2 = [12, 15] = 12 \cdot 15/(12, 15) = 180/3 = 60$; общие кратные: $M_2 = m_2 t = \{60, 120, 180,...\}$, $t \in Z$.

в) $m_3 = [4, 9] = 4 \cdot 9/(4, 9) = 36/1 = 36$; общие кратные: $M_3 = m_3 t = \{36, 72, 108,...\}$, $t \in Z$.

г) $m_4 = [15, 18]=15\ 18/(15, 18)=270/3=90$; общие кратные: $M_4 = m_4 t = \{90, 180, 270\ldots\}$, $t \in Z$.

д) $m_5=[21, 35]=21\ 35/(21, 35)=735/7=105$; общие кратные: $M_5 = m_5 t = \{105, 210, 315\ldots\}$, $t \in Z$.

е) $m_6=[42, 39]=42\ 39/(42, 39)=1638/3=546$; общие кратные: $M_6 = m_6 t = \{546, 1092, 1638\}$, $t \in Z$.

Решение к задаче 1.11.

а) $132300 = 2^2 \cdot 3^3 \cdot 5^2 \cdot 7^2$, $\varphi(132300) = 2 \cdot 1 \cdot 3^2 \cdot 2 \cdot 5 \cdot 4 \cdot 7 \cdot 6 = 30240$.

б) $588000 = 2^5 \cdot 3 \cdot 5^3 \cdot 7^2$, $\varphi(588000) = 2^4 \cdot 1 \cdot 1 \cdot 2 \cdot 5^2 \cdot 4 \cdot 7 \cdot 6 = 134400$.

в) $1620 = 2^2 \cdot 3^4 \cdot 5^1$, $\varphi(1620) = 2 \cdot 1 \cdot 3^3 \cdot 2 \cdot 5^0\ 4 = 432$.

г) $999 = 3^3\ 37^1$, $\varphi(999) = 3^2\ 2\ 37^0\ 36 = 648$.

д) $1044 = 2^2\ 3^2\ 29^1$, $\varphi(1044) = 2^1\ 1\ 3^1\ 2\ 29^0\ 28 = 336$.

е) $94 = 2^1\ 47^1$, $\varphi(94) = 2^0 \cdot 1 \cdot 47^0 \cdot 46 = 46$;

ж) $39 = 3^1\ 13^1$, $\varphi(39) = 3^0 \cdot 2 \cdot 13^0 \cdot 12 = 24$;

з) $72 = 2^3\ 3^2$, $\varphi(72) = 2^2 \cdot 1 \cdot 3 \cdot 2 = 24$;

и) $2310 = 2^1\ 3^1\ 5^1\ 7^1\ 11^1$, $\varphi(2310) = 2^0 \cdot 1 \cdot 3^0 \cdot 2 \cdot 5^0 \cdot 4 \cdot 7^0 \cdot 6 \cdot 11^0 \cdot 10 = 480$.

Решение к задаче 1.12.

а) $17 \equiv 2 \bmod 5$; б) $-11 \equiv -1 \bmod 5 \equiv 4 \bmod 5$;

в) $136 \equiv 1 \bmod 5$; г) $355 \equiv 0 \bmod 5$.

Решение к задаче 1.13.

а) $25 \equiv 1 \bmod 8$; б) $5 \equiv 1 \bmod 2$; в) $10 \equiv 3 \bmod 7$;

г) $-15 \equiv 6 \bmod 7$; д) $-10 \equiv 0 \bmod 2$; е) $-9 \equiv 3 \bmod 4$.

Решение к задаче 1.14.

а) $5 \equiv 1 \bmod 2$; б) $10 \equiv 0 \bmod 5$; в) $7 \equiv 7 \bmod 10$; г) $14 \equiv 2 \bmod 3$;

д) $-6 \equiv 4 \bmod 5$; е) $-20 \equiv 6 \bmod 13$; ж) $11 \equiv 4 \bmod 7$; з) $19 \equiv 6 \bmod 13$;

и) $10356 \equiv 3 \bmod 29$.

Решение к задаче 1.15.

а) $15 \equiv 5 \bmod 3$ – неверно. $15 \equiv 0 \bmod 3$

б) $28 \equiv 3 \bmod 5$ – верно;

в) $23 \equiv 4 \bmod 4$ – неверно. $23 \equiv 3 \bmod 4$;

г) $16 \equiv 2 \bmod 7$ – верно;

д) $3 \equiv 2 \bmod 2$ – неверно. $3 \equiv 1 \bmod 2$;

е) $12 \equiv 3 \bmod 3$ – верно.

Решение к задаче 1.16.

а) m=42. Найдем числа, взаимнопростые с модулем:

П = {1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41}.

Их количество $\varphi(42) = 12$.

б) m=39. Найдем числа, взаимнопростые с модулем:

П={1, 2, 4, 5, 7, 8, 10, 11, 14, 16, 17, 19, 20, 22, 23, 25, 28, 29, 31, 32, 34, 35, 37, 38}.

Их количество $\varphi(39) = 24$.

в) m=37. Найдем числа, взаимнопростые с модулем:

П={1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36}.

Их количество $\varphi(37) = 36$.

Решение к задаче 1.17.

а) $x^4+x+2 \equiv 0 \bmod 5$.

Полная система вычетов по модулю 5: {0, 1, 2, 3, 4}.

Решим сравнение полным перебором.

$f(0) = 2 \neq 0 \bmod 5$, $f(1) = 1+1+2 = 4 \neq 0 \bmod 5$, $f(2) = 16+2+2 = 20 \equiv 0 \bmod 5$, $f(3) = 81+3+2 = 86 \neq 0 \bmod 5$, $f(4) = 256+4+2 = 262 \neq 0 \bmod 5$.

Среди чисел 0,1,2,3,4 полной системы вычетов по модулю 5 сравнению удовлетворяет только $x = 2$, т.е. сравнение имеет одно решение.

Ответ: $x = 2$.

б) $32x \equiv 102 \bmod 123$.

Решим сравнение с помощью алгоритма Эвклида.

1. Определяем (a,m): $(32,123) = 1$. Сравнение имеет одно решение.

2. Выполняем алгоритм Евклида для 123/32:

– неполные частные $q_1 = 3$, $q_2 = 1$, $q_3 = 5$, $q_4 = 2$, $q_5 = 2$, $n = 5$;

– $P_1 = q_1 = 3$, $P_2 = 1 \cdot 3+1 = 4$, $P_3 = 5 \cdot 4+3 = 23$, $P_4 = 2 \cdot 23+4 = 50$.

3. Решение сравнения

$$x \equiv (-1)^4 P_4 b \bmod m \equiv 50 \cdot 102 \bmod 123 \equiv 57 \bmod 123.$$

4. Проверка: $32 \cdot 57 = 1824 \equiv 102 \bmod 123$.

5. Ответ: $x = 57$.

в) $111x \equiv 75 \bmod 321$.

1. Так как $(111,321) = d = 3$, то сравнение имеет три решения (с учетом того, что 75 делится на 3).

2. Делим на $d = 3$, получаем сравнение

$$37x \equiv 25 \bmod 107.$$

3. Выполняем алгоритм Евклида для 107/37:

	107	37
	74	$2=q_1$
37	33	
33		$1=q_2$
33	4	
32		$8=q_3$
4	1	
4		$4=q_4$
0		

Найдем $P_i = q_iP_{i-1}+P_{i-2}$ для $P_{-1} = 0$, $P_0 = 1$. Все результаты сведем в таблицу

i	0	1	2	3	4
q_i		2	1	8	4
P_i	1	2	3	26	107

Из таблицы:

$$n = 4,\ P_{n-1} = 26.$$

4. Определяем первое решение

$$x_1 \equiv (-1)^3 26 \cdot 25 \bmod 107 \equiv -26 \cdot 25 \equiv 99 \bmod 107.$$

5. Остальные решения:

$$x_2 = 99+107 = 206,\ x_3 = 206+107 = 313.$$

6. Проверка для $x_3 = 313$:

$$111\ 313 = 34743 \equiv 75 \bmod 321.$$

Ответ: $x_1 = 99$, $x_2 = 206$, $x_3 = 313$.

г) $81x \equiv 34 \bmod 95$.

1. Так как $(81,95) = d = 1$, то сравнение имеет одно решение.

2. Выполняем алгоритм Евклида для 95/81.

	95	81
	81	$1=q_1$
81	14	
70		$5=q_2$
11		
14	11	
11		$1=q_3$
11	3	
9		$3=q_4$
3	2	
2		$1=q_5$

_2	1
2	2=q_6
0	

Результаты деления по алгоритму Евклида и $P_i = q_iP_{i-1}+P_{i-2}$ для начальных условий $P_{-1} = 0$, $P_0 = 1$ сведем в таблицу

i	0	1	2	3	4	5	6
q_i		1	5	1	3	1	2
P_i		1	6	7	27	34	95

3.Определяем решение

$$x \equiv (-1)^5 \cdot 34 \cdot 34 \bmod 95 \equiv 79 \bmod 95.$$

4. Проверка для $x = 79$

$$81 \cdot 79 = 6399 \equiv 34 \bmod 95.$$

Ответ: $x = 79$.

д) $124x \equiv 88 \bmod 144$.

1. $(a, m) = 4$, $b = 88$ делится на 4. Значит, сравнение имеет четыре решения.

2. Делим все части сравнения на d=4:

$$31x = 22 \bmod 36;$$

3. Неполные частные от деления по алгоритму Евклида для 36/31 и $P_i = q_iP_{i-1}+P_{i-2}$ для начальных условий $P_{-1} = 0$, $P_0 = 1$ сведены в таблицу

i	0	1	2	3
q_i		1	6	5
P_i	1	1	7	36

Из таблицы: $n = 3$, $P_2 = 7$.

4. Первое решение:

$$x_1 = (-1)^2 \cdot 7 \cdot 22 \bmod 36 = 154 \bmod 36 = 10 \bmod 36;$$

5. Другие решения:

$$x_2 = x_1+36 = 46;$$
$$x_3 = x_2+36 = 82;$$
$$x_4 = x_3+36 = 118.$$

6. Проверка для $x_4 = 118$:

$$124 \cdot 118 = 14632 \equiv 88 \bmod 144.$$

Ответ: $x_1 = 10$, $x_2 = 46$, $x_3 = 82$, $x_4 = 118$.

е) $351x \equiv 99 \bmod 198$.

1. Так как $(351,198) = d = 9$, то сравнение имеет девять решений (с учетом того, что 99 делится на 9).

2. Делим все части сравнения на $d = 9$, получаем сравнение:

$$39x \equiv 11 \bmod 22.$$

3. Выполняем алгоритм Евклида для 22/39:

	_22	39
	0	0=q_1
_39	22	
22	1=q_2	

$$
\begin{array}{rl|l}
 & 22 & 17 \\
\hline
 & 17 & 1=q_3 \\
\hline
 17 & 5 & \\
\hline
 15 & 3=q_4 & \\
\hline
 5 & 2 & \\
\hline
 4 & 2=q_5 & \\
\hline
 2 & 1 & \\
\hline
 2 & 2=q_6 & \\
\hline
 0 & &
\end{array}
$$

Результаты деления по алгоритму Евклида и $P_i = q_iP_{i-1}+P_{i-2}$ для начальных условий $P_{-1} = 0$, $P_0 = 1$ сведем в таблицу

i	0	1	2	3	4	5	6
q_i		0	1	1	3	2	2
P_i	1	0	1	1	4	9	22

Из таблицы: $P_{n-1} = 9$, $n = 6$.

4. Определяем первое решение

$$x_1 \equiv (-1)^5 \cdot 9 \cdot 11 \bmod 22 \equiv -99 \bmod 22 \equiv 11 \bmod 22.$$

5. Остальные решения:

$$x_2 = 11+22 = 33,\ x_3 = 33+22 = 55,$$
$$x_4 = 55+22 = 77,\ x_5 = 77+22 = 99,$$
$$x_6 = 99+22 = 121,\ x_7 = 121+22 = 143,$$
$$x_8 = 143+22 = 165,\ x_9 = 165+22 = 187.$$

6. Проверка для $x_9 = 187$:

$$351 \cdot 187 = 65637 \equiv 99 \bmod 198.$$

Ответ: $x_1 = 11,\ x_2 = 33,\ x_3 = 55,\ x_4 = 77,\ x_5 = 99,\ x_6 = 121,\ x_7 = 143,\ x_8 = 165,\ x_9 = 187$.

Решение к задаче 1.18.

а) $134x \equiv 92 \bmod 152$.

1. $(a, m) = 2$, $b = 92$ делится на 2. Значит, сравнение имеет два решения.

2. Разделим все части сравнения на $d = 2$:

$$67x = 46 \bmod 76.$$

3. Результаты деления по алгоритму Евклида для 76/67 и $P_i = q_iP_{i-1}+P_{i-2}$ для начальных условий $P_{-1} = 0$, $P_0 = 1$ сведены в таблицу

i	0	1	2	3	4
q_i		1	7	2	4
P_i	1	1	8	17	76

Из таблицы:

$$n = 4,\ P_3 = 17.$$

4. Первое решение:

$$x_1 = (-1)^3 \cdot 17 \cdot 46 \bmod 76 = -782 \bmod 76 = 54 \bmod 76;$$

5. Второе решение

$$x_2 = x_1+76 = 130.$$

6. Проверка для $x_2 = 130$: $134 \cdot 130 = 17420 = 92 \bmod 152$.

Ответ: $x_1 = 54$; $x_2 = 130$.

б) $128x \equiv 34 \bmod 146$.

1. Так как $(128,146) = d = 2$, то сравнение имеет два решения (с учетом того, что 34 делится на 2).

2. Делим все части сравнения на $d = 2$, получаем сравнение:

$$64x \equiv 17 \bmod 73.$$

3. Выполняем алгоритм Евклида для 73/64:

_73	64	
64	1	$=q_1$
_64	9	
63	7	$=q_2$
_9	1	
9	9	$=q_3$
0		

Результаты деления по алгоритму Евклида и $P_i = q_iP_{i-1}+P_{i-2}$ для начальных условий $P_{-1} = 0$, $P_0 = 1$ сведены в таблицу

i	0	1	2	3
q_i		1	7	9
P_i	1	1	8	73

Из таблицы:

$$n = 3,\ P_{n-1} = 8.$$

4. Определяем первое решение

$$x_1 \equiv (-1)^2 \cdot 8 \cdot 17 \bmod 73 \equiv 63 \bmod 73\ .$$

5. Остальные решения:

$$x_2 = 63+73 = 136.$$

6. Проверка для $x_2 = 136$: $128 \cdot 136 = 17408 = 34 \bmod 146$.

Ответ: $x_1 = 63$; $x_2 = 136$.

в) $122x \equiv 96 \bmod 134$.

1. Так как $(122,134) = d = 2$, то сравнение имеет два решения (с учетом того, что 96 делится на 2).

2. Делим все части сравнения на $d = 2$, получаем сравнение:

$$61x = 48 \bmod 67.$$

3. Результаты деления по алгоритму Евклида для 67/61 и $P_i = q_iP_{i-1}+P_{i-2}$ для начальных условий $P_{-1} = 0$, $P_0 = 1$ сведены в таблицу

i	0	1	2	3
q_i		1	10	6
P_i	1	1	11	67

Из таблицы:

$$n = 3,\ P_{n-1} = 11.$$

4. Первое решение

$$x_1 = (-1)^2 \cdot 11 \cdot 48 \bmod 67 = 528 \bmod 67 = 59 \bmod 67.$$

5. Второе решение

$$x_2 = x_1+67 = 126;$$

6. Проверка для $x_2 = 126$: $122 \cdot 126 = 15372 = 96 \bmod 134$.

Ответ: $x_1 = 59$; $x_2 = 126$.

г) $126x \equiv 38 \bmod 142$.

1. Так как (126,142) = d = 2, то сравнение имеет два решения (с учетом того, что 38 делится на 2).

2. Делим все части сравнения на d = 2, получаем сравнение:

$$63x = 19 \bmod 71;$$

3. Определяем q_i по алгоритму Евклида для 71/63 и $P_i = q_iP_{i-1}+P_{i-2}$ для начальных условий $P_{-1} = 0$, $P_0 = 1$

i	0	1	2	3	4
q_i		1	7	1	7
p_i	1	1	8	9	71

4. Первое решение:

$$x_1 = (-1)^3 \cdot 9 \cdot 19 \bmod 71 = -171 \bmod 71 = 42 \bmod 71.$$

5. Второе решение:

$$x_2 = x_1+71 = 113.$$

6. Проверка для x_2 = 113: $126 \cdot 113 = 14238 = 38 \bmod 142$.

Ответ: $x_1 = 42$; $x_2 = 113$.

д) $130x \equiv 58 \bmod 144$.

1. Так как (144,130) = d = 2, то сравнение имеет два решения (с учетом того, что 58 делится на 2).

2. Делим все части сравнения на d = 2, получаем сравнение:

$$65x = 29 \bmod 72;$$

3. Определяем q_i по алгоритму Евклида для 72/65 и $P_i = q_iP_{i-1}+P_{i-2}$ для начальных условий $P_{-1} = 0$, $P_0 = 1$

i	0	1	2	3	4
q_i		1	9	3	2
P_i	1	1	10	31	72

Из таблицы:

$$n = 4,\ P_{n-1} = P_3 = 31.$$

4. Определяем первое решение сравнения:

$$x_1 = (-1)^3 \cdot 31 \cdot 29 \equiv -899 \bmod 72 \equiv 37 \bmod 72.$$

5. Второе решение:

$$x_2 = x_1+72 = 37+72 = 109.$$

6. Проверка x_2 = 109: $130 \cdot 109 = 14170 \equiv 58 \bmod 144$.

Ответ: $x_1 = 37$, x_2=109.

е) $132x \equiv 82 \bmod 142$.

1. Так как (142,132) = d = 2, то сравнение имеет два решения (с учетом того, что 82 делится на 2).

2. Делим все части сравнения на d = 2, получаем сравнение:

$$66x = 41 \bmod 71.$$

3. Определяем q_i по алгоритму Евклида для 71/66 и $P_i = q_iP_{i-1}+P_{i-2}$ для начальных условий $P_{-1} = 0$, $P_0 = 1$

i	0	1	2	3
q_i		1	13	5
P_i	1	1	14	71

Из таблицы:

$$n = 3,\ P_{n-1} = P_2 = 14.$$

4. Определяем первое решение сравнения:

$$x_1 = (-1)^2 \cdot 14 \cdot 41 \equiv 574 \bmod 71 \equiv 6 \bmod 71.$$

5. Второе решение:

$$x_2 = x_1 + 71 = 6 + 71 = 77.$$

6. Проверка $x_2 = 77$: $132 \cdot 77 \equiv 10164 = 82 \bmod 142$.

Ответ: $x_1 = 6$, $x_2 = 77$.

ж) $152x \equiv 29 \bmod 211$.

1. Так как $(152,211) = d = 1$, то сравнение имеет одно решение.

2. Определяем q_i по алгоритму Евклида для 211/152 и $P_i = q_i P_{i-1} + P_{i-2}$ для начальных условий $P_{-1} = 0$, $P_0 = 1$

i	0	1	2	3	4	5	6	7	8
q_i		1	2	1	1	2	1	3	2
P_i	1	1	3	4	7	18	25	93	211

Из таблицы:

$$n = 8,\ P_{n-1} = P_7 = 93.$$

3. Определяем решение сравнения

$$x = (-1)^{n-1} P_{n-1} b \bmod m = -93 \cdot 29 \equiv -165 \bmod 211 \equiv 46 \bmod 211.$$

4. Проверка $x = 46$: $152 \cdot 46 = 6992 \equiv 29 \bmod 211$.

Ответ: $x = 46$.

з) $579x \equiv 273 \bmod 462$.

1. Так как $a = 579 > m = 462$, то определим $579 \equiv 117 \bmod 462$, получаем эквивалентное уравнение $117x \equiv 273 \bmod 462$.

2. $a = 117 = 3 \cdot 3 \cdot 13$, $m = 462 = 2 \cdot 3 \cdot 7 \cdot 11$, $b = 273 = 3 \cdot 7 \cdot 13$. $(a,m) = 3$. Следовательно, сравнение имеет три решения.

3. Делим все части сравнения на $d = 3$, получаем сравнение:

$$39x \equiv 91 \bmod 154.$$

4. Выполняем алгоритм Евклида для 154/39, и $P_i = q_i P_{i-1} + P_{i-2}$ для начальных условий $P_{-1} = 0$, $P_0 = 1$

i	0	1	2	3	4
q_i		3	1	18	2
P_i	1	3	4	75	154

Из таблицы:

$$n = 4,\ P_3 = 75$$

5. Определяем первое решение x_1:

$x_1 = (-1)^3 \cdot 75 \cdot 91 \bmod 154 = -6825 \bmod 154 \equiv -49 \bmod 154 \equiv 105 \bmod 154$.

6. Остальные решения

$$x_2 = 105 + 154 = 259,$$
$$x_3 = 259 + 154 = 413.$$

7. Проверка для $x_3 = 413$: $579 \cdot 413 = 239127 \equiv 273 \bmod 462$.

Ответ: $x_1 = 105$, $x_2 = 259$, $x_3 = 413$.

Решение к задаче 1.19.

а) $a_1 = 1$; б) $a_2 = 2$; в) $a_3 = 3$; г) $a_4 = 4$.

1) Проведем последовательное возведение в степень элементов a_i ($i = \overline{1,4}$) и определим их показатели (периоды):

а) $1^1 \equiv 1 \bmod 5$, т.е. $\varepsilon_1 = 1$;

б) $2^2 = 4$, $2^3 = 8 \equiv 3 \bmod 5$, $2^4 = 16 \equiv 1 \bmod 5$, т.е. $\varepsilon_2 = 4$;

в) $3^2 = 9 \equiv 4 \bmod 5$, $3^3 = 27 \equiv 2 \bmod 5$, $3^4 = 81 \equiv 1 \bmod 5$, т.е. $\varepsilon_3 = 4$;

г) $4^2 = 16 \equiv 1 \bmod 5$, т.е. $\varepsilon_4 = 2$.

2) При дальнейшем возведении элементов a_i в последовательные степени наблюдается их периодическая повторяемость по модулю 5; для $a_3 = 3$: $3^5 \equiv 3 \bmod 5 \equiv 3^1$, $3^6 \equiv 3^2 \bmod 5$, $3^7 \equiv 3^3 \bmod 5$, $3^8 \equiv 3^4 \bmod 5 \equiv 1 \bmod 5$ и т.д.

Ответ: $\varepsilon_1 = 1$, $\varepsilon_2 = 4$, $\varepsilon_3 = 4$, $\varepsilon_4 = 2$.

Решение к задаче 1.20.

$a_1 = 1$, $a_2 = 2$,..., $a_6 = 6$.

1. Проведем последовательное возведение в степень элементов a_i ($i = \overline{1,6}$) и определим их показатели (периоды):

а) $1^1 \equiv 1 \bmod 7$, т.е. $\varepsilon_1 = 1$;

б) $2^2 = 4$, $2^3 = 8 \equiv 1 \bmod 7$, т.е. $\varepsilon_2 = 3$;

в) $3^2 = 9 \equiv 2 \bmod 7$, $3^3 = 27 = 6 \bmod 7$, $3^4 = 81 \equiv 4 \bmod 7$, $3^5 = 243 \equiv 5 \bmod 7$, $3^6 = 729 \equiv 1 \bmod 7$, т.е. $\varepsilon_3 = 6$;

г) $4^2 = 16 \equiv 2 \bmod 7$, $4^3 = 64 = 1 \bmod 7$, т.е. $\varepsilon_4 = 3$;

д) $5^2 = 25 = 3 \bmod 7$, $5^3 = 125 = 6 \bmod 7$, $5^4 = 625 = 2 \bmod 7$, $5^5 = 3125 = 3 \bmod 7$, $5^6 = 15625 = 1 \bmod 7$, т.е. $\varepsilon_5 = 6$;

е) $6^2 = 36 = 1 \bmod 7$, т.е. $\varepsilon_6 = 2$.

Ответ: $\varepsilon_1 = 1$, $\varepsilon_2 = 3$, $\varepsilon_3 = 6$, $\varepsilon_4 = 3$, $\varepsilon_5 = 6$, $\varepsilon_6 = 2$.

Решение к задаче 1.21.

1. Определяем элементы приведенной системы вычетов по модулю 9:

$$П = \{1, 2, 4, 5, 7, 8\},\ \varphi(m) = \varphi(9) = 6.$$

2. Вычисляем распределение показателей по элементам (это есть делители числа 6: 1, 2, 3, 6):

$1^1 \equiv 1 \bmod 9$, $\varepsilon_1 = 1$;

$2^2 = 4$, $2^3 = 8$, $2^4 \equiv 7 \bmod 9$, $2^5 \equiv 5 \bmod 9$, $2^6 \equiv 1 \bmod 9$, $\varepsilon_2 = 6$;

$4^2 = 16 \equiv 7 \bmod 9$, $4^3 \equiv 1 \bmod 9$, $\varepsilon_4 = 3$,

$5^2 = 25 \equiv 7 \bmod 9$, $5^3 \equiv 8 \bmod 9$, $5^4 \equiv 4 \bmod 9$, $5^5 \equiv 2 \bmod 9$,

$5^6 \equiv 1 \bmod 9$, $\varepsilon_5 = 6$;

$7^2 \equiv 4 \bmod 9$, $7^3 \equiv 1 \bmod 9$, $\varepsilon_7 = 3$,

$8^2 = 64 \equiv 1 \bmod 9$, $\varepsilon_8 = 2$.

Ответ: $\varepsilon_1 = 1$, $\varepsilon_2 = 6$, $\varepsilon_4 = 3$, $\varepsilon_5 = 6$, $\varepsilon_7 = 3$, $\varepsilon_8 = 2$.

Решение к задаче 1.22.

1. Определяем элементы приведенной системы вычетов по модулю 10:

$П = \{1, 3, 7, 9\}$, $\varphi(m) = \varphi(10)=4$.

2. Вычисляем распределение показателей по элементам (это есть делители числа 4: 1, 2, 4):

$1^1 \equiv 1 \bmod 10$, $\varepsilon_1 = 1$;

$3^3 \equiv 7 \bmod 10$, $3^4 \equiv 1 \bmod 10$, $\varepsilon_3 = 4$;

$7^2 \equiv 9 \bmod 10$, $7^3 \equiv 3 \bmod 10$, $7^4 \equiv 1 \bmod 10$, $\varepsilon_7 = 4$;

$9^2 \equiv 1 \bmod 10$, $\varepsilon_9 = 2$;

Ответ: $\varepsilon_1 = 1$, $\varepsilon_3 = 4$, $\varepsilon_7 = 4$, $\varepsilon_9 = 2$.

Решение к задаче 1.23.

а) m=9.

a_1=4; $4^2 = 7 \bmod 9$, $4^3 = 1 \bmod 9$; $\varepsilon_1 = 3$.

a_2=2; $2^4 = 7 \bmod 9$, $2^5 = 5 \bmod 9$, $2^6 = 1 \bmod 9$; $\varepsilon_2 = 6$.

Ответ: $\varepsilon_1 = 3$, $\varepsilon_2 = 6$.

б) m=7.

a_1=2; $2^2 = 4 \bmod 7$, $2^3 = 1 \bmod 7$, $\varepsilon_1 = 3$.

a_2=3; $3^2 = 2 \bmod 7$, $3^3 = 6 \bmod 7$, $3^4 = 4 \bmod 7$, $3^5 = 5 \bmod 7$, $3^6 = 1 \bmod 7$; $\varepsilon_2 = 6$.

Ответ: $\varepsilon_1 = 3$, $\varepsilon_2 = 6$.

Решение к задаче 1.24.

а) m=3; $\varphi(m) = \varphi(3) = 2$; α=2.

Ответ: α=2.

б) m=4; $\varphi(m) = \varphi(4) = 2$; α=3.

Ответ: α=3.

Решение к задаче 1.25.

В качестве основания выберем наименьший первообразный корень $\alpha = 2$. Находим степени первообразного корня по модулю $p = 13$:

$2^0 = 1$	$2^4 = 3$	$2^8 = 9$
$2^1 = 2$	$2^5 = 6$	$2^9 = 5$
$2^2 = 4$	$2^6 = 12$	$2^{10} = 10$
$2^3 = 8$	$2^7 = 11$	$2^{11} = 7$.

Полученные результаты сведены в табл.1.1.

Таблица 1.1

$p = 13$, $p-1 = 2^2 \cdot 3$, $\alpha = 2$

N	0	1	2	3	4	5	6	7	8	9
0		0	1	4	2	9	5	11	3	8
1	10	7	6							

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	3	6	12	11	9	5
1	10	7								

В левой части таблицы определяем индекс по числу, в правой – число по индексу. Номер строки в таблице указывает число десятков, номер столбца – число единиц числа (индекса). На пересечении строки и столбца помещается соответствующий индекс (число). Например, $\text{ind}_2 12$ находится на пересечении первой строки и второго столбца левой части табл.1.1, т.е. $\text{ind}_2 12 = 6$. Индексу $I = 11$ соответствует число $a = 7$, находящееся на пересечении первой строки и первого столбца правой части табл.1.1.

Решение к задаче 1.26.

В качестве основания выберем наибольший первообразный корень $\alpha = 11$. Находим степени первообразного корня по модулю $p = 13$:

$11^0 = 1$; $11^1 = 11$; $11^2 = 4$; $11^3 = 5$;$11^4 = 3$; $11^5 = 7$;$11^6 = 12$; $11^7 = 2$; $11^8 = 9$;

$11^9 = 8$; $11^{10} = 10$; $11^{11} = 6$.

Полученные результаты сведены в табл.1.2.

Таблица 1.2

$p = 13$, $p-1 = 2^2 \cdot 3$, $\alpha = 11$

N	0	1	2	3	4	5	6	7	8	9
0		0	7	4	2	3	11	5	9	8
1	10	1	6							

I	0	1	2	3	4	5	6	7	8	9
0	1	11	4	5	3	7	12	2	9	8
1	10	6								

В левой части таблицы определяем индекс по числу, в правой – число по индексу. Номер строки в таблице указывает число десятков, номер столбца – число единиц числа (индекса). На пересечении строки и столбца помещается соответствующий индекс (число). Например, $\text{ind}_{11}12$ находится на пересечении первой строки и второго столбца левой части табл.1.2, т.е. $\text{ind}_{11}12 = 6$. Индексу $I = 11$ соответствует число $a = 6$, находящееся на пересечении первой строки и первого столбца правой части табл.1.2.

Решение к задаче 1.27.

Показатели элементов, в том числе и для $\alpha = 5$, приведенной системы вычетов $\Pi = \{1,2,4,5,7,8\}$ по модулю $m = 9$ получены в задаче 21:

$5^0 = 1$, $5^1 = 5$, $5^2 = 7$, $5^3 = 8$, $5^4 = 4$, $5^5 = 2$, $5^6 = 1$, $\varepsilon_5 = \varphi(9) = 6$.

Отсюда определяем индексы всех элементов приведенной системы вычетов:

$$I_1 = \text{ind}_5 1 = 0;\ I_2 = \text{ind}_5 2 = 5;\ I_4 = \text{ind}_5 4 = 4;$$
$$I_5 = \text{ind}_5 5 = 1;\ I_7 = \text{ind}_5 7 = 2;\ I_8 = \text{ind}_5 8 = 3.$$

Решение к задаче 1.28.

а) $m_1 = 10$.

1. $\varphi(10) = 4$.

2. Наибольший первообразный корень найдем среди элементов приведенной системы вычетов (см. задание 22), тот, для которого $\varepsilon = \varphi(10) = 4$:

$$\alpha = 7,\ \varepsilon_7 = 4.$$

3. Показатели элементов, в том числе и для $\alpha = 7$, приведенной системы вычетов $\Pi = \{1, 3, 7, 9\}$ по модулю $m = 10$ получены в задаче 22:

$$7^0 \equiv 1,\ 7^1 \equiv 7,\ 7^2 \equiv 9,\ 7^3 \equiv 3,\ 7^4 \equiv 1,\ \varepsilon_7 = \varphi(10) = 4.$$

Определяем индексы всех элементов приведенной системы вычетов:

$$I_1 = \text{ind}_7 1 = 0;\ I_3 = \text{ind}_7 3 = 3;\ I_7 = \text{ind}_7 7 = 1;\ I_9 = \text{ind}_7 9 = 2.$$

Ответ: $I_1 = \text{ind}_7 1 = 0$; $I_3 = \text{ind}_7 3 = 3$; $I_7 = \text{ind}_7 7 = 1$; $I_9 = \text{ind}_7 9 = 2$.

б) $m_2 = 12$.

1. $\varphi(12) = 4$.

2. Наибольший первообразный корень найдем среди элементов приведенной системы вычетов $\Pi = \{1, 5, 7, 11\}$, тот, для которого $\varepsilon = \varphi(12) = 4$:

$$11^0 \equiv 1,\ 11^1 \equiv 11,\ 11^2 \equiv 1,\ \varepsilon_{11} = 2;$$
$$7^0 \equiv 1,\ 7^1 \equiv 7,\ 7^2 \equiv 1,\ \varepsilon_7 = 2;$$
$$5^0 \equiv 1,\ 5^1 \equiv 5,\ 5^2 \equiv 1,\ \varepsilon_5 = 2;$$
$$1^0 \equiv 1,\ 1^1 \equiv 1,\ \varepsilon_1 = 1.$$

Первообразных корней по модулю 12 не существует.

Ответ: Первообразных корней по модулю 12 не существует.

2 ОСНОВНЫЕ ПОНЯТИЯ И ОПРЕДЕЛЕНИЯ ТЕОРИИ ПОЛЕЙ ГАЛУА

2.1 Группа, подгруппа, циклическая группа

Современная теория помехоустойчивого кодирования основана на таких понятиях алгебры, как группы и конечные поля. Особое значение имеют бинарные операции.

Определение. Б и н а р н о й о п е р а ц и е й * называется такая операция, которая каждой упорядоченной паре элементов данного множества ставит в соответствие третий элемент этого множества.

Таким образом, бинарная операция на множестве K – это отображение $K\times K\to K$, где декартово произведение $K\times K$ суть множество всех упорядоченных пар элементов из заданного множества K.

Наряду с обычными операциями сложения и умножения в качестве бинарных операций часто используют две специальные операции $\oplus$ и $\otimes$ со свойствами, аналогичными сложению и умножению вещественных чисел, в частности, допускающими выполнение обратных операций типа вычитания и деления (кроме деления на нуль). Данные бинарные операции называются м о д у л ь н ы м и сложением и умножением и определяются соотношениями:

– сложение $\oplus$ по модулю p:

$$a \oplus b = (a+b) \bmod p = \text{rest}\left[\frac{a+b}{p}\right];$$

– умножение $\otimes$ по модулю p:

$$a \otimes b = (a \cdot b) \bmod p = \text{rest}\left[\frac{a \cdot b}{p}\right],$$

где rest[...] означает остаток от деления на простое число p суммы $a+b$ или произведения $a \cdot b$ – обычных арифметических операций сложения и умножения.

Определение. Г р у п п о й называется множество G, на котором задана бинарная операция * и выполняется ряд аксиом:

1) замкнутости: любой паре элементов $a, b \in G$ ставится в соответствие третий элемент $c \in G$:

$$a, b \in G \Rightarrow c = a*b \in G;$$

2) ассоциативности:

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

3) существования нейтрального элемента e, не изменяющего любого элемента a, участвующего вместе с e в бинарной операции:

$$a*e = e*a = a, \forall a \in G;$$

4) существования для любого ненулевого элемента $a \in G$ обратного элемента a^{-1}, обращающего с помощью бинарной операции a в e:

$$a*a^{-1} = a^{-1}*a = e, \forall a \in G.$$

Группа называется коммутативной или абелевой, если групповая бинарная операция * является коммутативной:

$$a*b = b*a,\ \forall a, b \in G.$$

Далее речь будет идти только о коммутативных группах. Бинарная операция в абелевых группах задается в виде операций сложения или умножения.

Если бинарной операции * соответствует операция сложения +, то группа называется аддитивной и обозначается G_+. При этом нейтральный элемент $e = 0$ ($a+0 = 0+a = a$), а обратный элемент a^{-1} называется противоположным или аддитивно обратным и обозначается $-a$ ($a+(-a) = 0$).

Если бинарной операции * соответствует операция умножения (обозначается × или ·), то группа называется мультипликативной группой $G_\times$. При этом нейтральный элемент $e = 1$ ($a\times 1 = 1\times a = a$), а для мультипликативно обратного элемента выполняется равенство $a\times a^{-1} = 1$.

Простейшими примерами абелевых групп служат: множество целых чисел с обычной операцией сложения; множество рациональных чисел, за исключением нуля, с обычной операцией умножения.

Определение. П о д г р у п п о й группы G называется подмножество $H \in G$, являющееся группой относительно той же бинарной операции *.

Подгруппа всегда содержит нейтральный элемент e группы, так как он является также нейтральным элементом любой ее подгруппы.

Если группа G состоит из конечного числа L элементов, ее называют конечной, а число L – порядком группы.

Для конечной мультипликативной группы $G_\times$ вводится понятие натуральной степени a^n, где n – нуль или натуральное число:

$$a^0 = 1,\ a\cdot a = \underbrace{a^2, \ldots,}$$
$$a\cdot a\cdot \ldots \cdot a = a^n.$$

Определение. Конечная мультипликативная группа $G_\times$ с операцией $\otimes$ называется ц и к л и ч е с к о й , порожденной элементом a, если каждый элемент $b \in G_\times$ есть некоторая натуральная степень элемента a, т. е. $b = a^j$ (j – натуральное число).

Для конечных групп используется обозначение $G(p)$, где p – простое число. Конечная аддитивная группа обозначается $G_+(p)$ и имеет порядок $L = p$. Конечная мультипликативная группа обозначается $G_\times(p)$ и имеет порядок $L = p-1$ (исключается нулевой элемент).

Определение. П е р и о д о м (п о р я д к о м) э л е м е н т а a конечной мультипликативной группы $G_\times(p)$ порядка $L = p-1$ называется минимальное натуральное число ε, для которого выполняется равенство $a^\varepsilon \equiv 1 \bmod L$. В этом случае циклическая группа (подгруппа), порожденная элементом a, будет иметь порядок $L = \varepsilon$:

$$G = \{1 = a^0, a^1, a^2, \ldots, a^{\varepsilon-1}\},\ a^h = 1,$$

где $h = i\varepsilon$, i – произвольное целое число.

Справедлива следующая теорема выдающегося французского математика Ж. Лагранжа (1736 – 1813).

Теорема. Период (порядок) ε любого элемента a произвольной конечной группы является делителем порядка L этой группы, т. е. $\varepsilon | L$ (ε делит L без остатка).

Определение. Примитивным элементом α циклической группы называется элемент, последовательные степени которого α^i соответствуют всем элементам группы.

Примитивный элемент обладает максимальным периодом ε_{max}, равным порядку L группы, и может быть использован для построения циклической группы $G_{\times}(p)$.

2.2 Конечное поле

Определение. Полем F называется множество, удовлетворяющее следующим аксиомам:

1) все элементы поля F образуют аддитивную абелеву группу с операцией сложения $a + b = c$;

2) все элементы F, кроме нулевого, образуют мультипликативную абелеву группу с операцией умножения $a \cdot b = b \cdot a = d$;

3) умножение дистрибутивно относительно сложения, т.е. для любых трех элементов a, b, c из F выполняется равенство $(a+b)c = ac+bc$.

Таким образом, поле представляет собой объединение аддитивной и мультипликативной групп с заданием двух бинарных операций, наличием двух нейтральных элементов – нуля и единицы, а также аддитивно и мультипликативно обратных элементов.

Определение. Поле, содержащее конечное число элементов q, называется конечным полем и обозначается GF(q) (GF означает Galois Field – поле Галуа). Порядком конечного поля называется число элементов поля.

2.2.1 Простое поле

Элементарным примером конечного поля является простое поле, элементами которого являются целые числа – вычеты по модулю простого числа p.

Определение. Пусть x и y – произвольные целые числа и m – натуральное число. Тогда число x сравнимо с y по модулю m (обозначается $x \equiv y (\mathrm{mod}\ m)$), если разность $x–y$ делится на m без остатка, т.е. если $x = y + km$ для некоторого целого числа k.

Из примеров видно, что сравнивать по модулю можно как положительные, так и отрицательные целые числа. Операция сравнения по модулю числа m равносильна нахождению остатка от деления заданного числа на число m. В качестве остатка целесообразно выбирать наименьшее целое положительное число.

Все целые числа x такие, что $x \equiv r (\mathrm{mod}\ m)$ при фиксированном r, т. е. числа, которые дают при делении на m остаток r, образуют класс чисел (или класс вычетов) по модулю m, который обозначается через $\{r\}$ или $r (\mathrm{mod}\ m)$. Все числа класса можно получить, если в форме $mk+r$ заставить k пробегать все целые числа. Соответственно для m различных значений r имеем m классов чисел по модулю m. Любое число класса называется вычетом по модулю m по отношению ко всем числам этого класса.

Определение. П р о с т ы м п о л е м GF(p) называется конечное поле порядка p (p – простое число), образованное полной системой вычетов по модулю числа p. Число p называется х а р а к т е р и с т и к о й поля.

Удобным способом задания простого поля является табличный. Для каждой бинарной операции строится таблица, называемая таблицей групповой операции или таблицей Кэли группы.

Бинарные операции сложения и умножения можно представить в следующем виде:

1) сложение по модулю p:

$$a \oplus b = \begin{cases} a+b, & \text{если } a+b < p; \\ a+b-p, & \text{если } a+b \geq p; \end{cases}$$

2) умножение по модулю p:

$$a \otimes b = \begin{cases} ab, & \text{если } ab < p; \\ \text{rest}\left[(ab) : p\right], & \text{если } ab \geq p, \end{cases}$$

где $\text{rest}\left[(ab) : p\right]$ – остаток от деления ab на p.

Даные операции называют модульными операциями и обозначают $\oplus$ и $\otimes$ соответственно.

Далее для простоты модульные операции обозначаются без кружочка, если их смысл ясен из контекста.

Любая аддитивная группа $G_+(m)$ с модульным сложением является циклической группой, а элемент 1 – порождающим эту группу. Следовательно, операция модульного сложения обратима, и можно составить таблицы модульного вычитания:

а) $G_+ = \{0,1\}$, $m = 2$ б) $G_+ = \{0,1,2\}$, $m = 3$ в) $G_+ = \{0,1,2,3\}$, $m = 4$

⊖	0	1
0	0	1
1	1	0

⊖	0	1	2
0	0	2	1
1	1	0	2
2	2	1	0

⊖	0	1	2	3
0	0	3	2	1
1	1	0	3	2
2	2	1	0	3
3	3	2	1	0

Сравнение таблиц сложения и вычитания показывает, что для $m = 2$ они совпадают, т.е. в поле GF(2) операции сложения и вычитания по mod 2 эквивалентны. Для $m > 2$ элементы строк таблиц вычитания располагаются в противоположном порядке по отношению к таблицам сложения.

Аналогично операции модульного вычитания для аддитивной группы поля можно определить операцию модульного деления для мультипликативной группы поля. Модульное деление на ненулевой элемент $a \in$ GF(p) равносильно модульному умножению на мультипликативно обратный элемент a^{-1}.

2.2.2 Расширенное поле GF(p^n)

Аналогично сравнению целых чисел по модулю m можно определить операцию сравнения для полиномов над полем GF(p).

Определение. Полином $A(x)=\sum_{i=0}^{n} a_i x^i$ называется полиномом над полем GF(p), если его коэффициенты a_i принадлежат полю GF(p). Степенью полинома $A(x)$ называется наибольшее число n такое, что $a_n \neq 0 (\mathrm{mod}\ p)$.

Определение. Пусть $A(x)$, $B(x)$ и $F(x)$ – полиномы над полем GF(p). Тогда полином $A(x)$ сравним с $B(x)$ по модулю $F(x)$, т. е.

$$A(x) \equiv B(x) \bmod F(x),$$

если разность $A(x)–B(x)$ делится на $F(x)$ без остатка, т. е.

$$A(x) = B(x)+K(x)\cdot F(x)$$

для некоторого полинома $K(x)$.

Все операции в сравнениях выполняются еще и по модулю p, что отмечается записью

$$A(x) \equiv B(x) \mathrm{modd}(F(x),p),$$

которая означает, что полином $A(x)$ сравним с полиномом $B(x)$ по двойному модулю ($F(x)$, p).

Деление полинома на полином выполняется в «столбик» с заменой операции вычитания на операцию вычитания по модулю p. В качестве результата выбирается остаток $R(x)$, степень которого меньше степени делителя $F(x)$. Для случая $p = 2$ операции сложения и вычитания эквивалентны.

В дальнейшем для упрощения записи вместо знака сравнения по модулю «≡» будем использовать знак равенства «=», а вместо обозначения сравнения полиномов по двойному модулю modd ($F(x)$,p) – обозначение mod $F(x)$, если их смысл ясен из контекста.

Все полиномы $A(x)$ над полем GF(p) такие, что $A(x) \equiv R(x)(\mathrm{modd}\ F(x),\ p)$ при фиксированном $R(x)$, т. е. полиномы, которые дают при делении на $F(x)$ остаток $R(x)$, образуют класс полиномов (класс вычетов) по двойному модулю ($F(x)$, p), который обозначают через $\{R(x)\}$ или $R(x)$ modd ($F(x)$, p).

Если $F(x)$ – полином степени n над полем GF(p), то всевозможные остатки $R(x)$ – полиномы степени не выше n–1:

$$R(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + ... + a_1 x + a_0,$$

где $a_i \in$ GF(p), $i = \overline{0, n-1}$ – элементы простого поля.

Из данного выражения следует, что существует точно p^n различных полиномов $R(x)$. Соответственно, имеется p^n классов вычетов по двойному модулю ($F(x)$, p). Любой полином класса называется вычетом по двойному модулю ($F(x)$, p) по отношению ко всем полиномам этого класса.

Определение. Полином $f(x)$ степени $n \geq 1$ с коэффициентами из поля GF(p) неприводим над полем GF(p), если он не может быть представлен в виде произведения полиномов меньших степеней также с коэффициентами из GF(p).

Если из каждого класса взять по одному вычету, то получим полную систему вычетов. Обычно в качестве полной системы вычетов используют полиномы степени не выше n–1. Полная система вычетов по двойному модулю ($f(x)$, p), где $f(x)$ – полином, неприводимый над GF(p) и p – простое число, удовлетворяет всем аксиомам поля. Аналогично понятию простого поля как полной системы вычетов по модулю простого числа p вводится понятие расширенного поля GF(p^n).

Определение. Расширенным полем или расширением степени n простого поля GF(p) называют конечное поле GF(p^n), образованное полной системой вычетов по двойному модулю ($f(x)$, p) и содержащее p^n элементов.

В отличие от простого поля GF(p) элементами расширенного поля GF(p^n) являются уже не числа, а полиномы степени не выше n–1 с коэффициентами из GF(p).

Требование неприводимости полинома $f(x)$ степени n для расширенного поля GF(p^n) аналогично требованию простоты числа p для простого поля GF(p). В обоих случаях невыполнение этого требования ведет к невыполнению аксиомы существования обратного элемента для некоторых элементов поля.

2.3 Формы представления элементов поля Галуа

При рассмотрении мультипликативной группы были введены понятия натуральной степени элемента a и его периода (порядка) ε, а также понятие примитивного элемента α.

Наиболее продуктивным с точки зрения анализа мультипликативной структуры является способ построения поля на основе последовательного возведения в степень примитивного элемента α. Напомним, что примитивный элемент обладает максимальным периодом, равным порядку мультипликативной группы поля $\varepsilon_{max} = p^n-1$.

В общем случае показатели степеней элементов поля сравниваются по модулю $L = p^n-1$, равному порядку мультипликативной группы $G_\times$ поля GF(p^n).

При решении задач построения и преобразования полей в настоящее время используются следующие формы представления элементов поля: целочисленная, степенная, полиномиальная, векторная.

Определение. Форма представления элементов поля GF(p^n) называется:

1) степенной, если элементы представлены степенью α^i ($i = \overline{0, p^n-2}$) примитивного элемента α, нулевой элемент $0 = \alpha^{-\infty}$;

2) целочисленной, если элементы представлены целым неотрицательным числом от 0 до p^n–1;

3) полиномиальной, если элементы представлены всевозможными полиномами степени не выше n–1 с коэффициентами из простого поля GF(p);

4) векторной, если элементы представлены в виде векторов размерности n, координаты которых принимают значения из простого поля GF(p).

В качестве иллюстрации на следующей странице приведена таблица различных форм представления элементов поля GF(2^3), $f(x) = x^3+x+1$, $\alpha = a$.

Целочисленная	Степенная	Полиномиальная	Векторная
0	$\alpha^{-\infty}$	0	0 0 0
1	α^{0}	1	0 0 1
2	α^{1}	a	0 1 0
3	α^{2}	a^2	1 0 0
4	α^{3}	a+1	0 1 1
5	α^{4}	a^2+a	1 1 0
6	α^{5}	a^2+a+1	1 1 1
7	α^{6}	a^2+1	1 0 1

Целочисленная форма представления используется для компактной записи элементов поля, при составлении таблиц сложения и умножения и программ для ПЭВМ. Кроме того, наряду со степенной формой представления применяется при выполнении операции умножения. При операции сложения элементов поля целесообразно применять полиномиальную и векторную формы.

2.4 Примитивные полиномы и периоды элементов полей Галуа

Определение. Примитивным полиномом в поле GF(p^n) называется неприводимый полином степени n, одним из корней которого является примитивный элемент.

Понятие примитивного полинома является более узким по сравнению с неприводимым полиномом. Любой примитивный полином является неприводимым, но произвольный неприводимый над полем GF(p) полином не обязательно является примитивным. Отличие неприводимого и примитивного полиномов одинаковой степени n заключается в периоде корней этих полиномов. У примитивного полинома корнями являются примитивные элементы с максимальным периодом $\varepsilon_{max} = L = p^n - 1$, равным порядку мультипликативной группы поля. Корни неприводимого, но не примитивного полинома имеют период $\varepsilon < \varepsilon_{max}$, причем ε обязательно является делителем ε_{max}.

Для определения периода произвольного элемента a поля GF(p^n) можно поступить следующим образом: выполнять его последовательное возведение в степень i до тех пор, пока не выполнится условие $a^i \equiv 1$ modd ($f(x)$,p). Тогда период элемента $\varepsilon(a) = i$.

Более продуктивный способ определения периода элемента дает следующая теорема.

Теорема. Если период элемента a равен ε, то период элемента a^k определяется выражением

$$\varepsilon(a^k) = \frac{\varepsilon}{\text{НОД}(\varepsilon, k)},$$

где НОД(ε, k) – наибольший общий делитель чисел ε и k.

При степенной форме представления элементов поля, построенного по примитивному элементу α, имеющему период $\varepsilon_{max} = p^n - 1$, периоды всех элементов поля вычисляются в соответствии с выражением

$$\varepsilon(\alpha^i) = \frac{p^n - 1}{\text{НОД}(i, p^n - 1)}.$$

Число элементов, имеющих период ε, определяется выражением

$$N_\varepsilon = \varphi(\varepsilon),$$

где $\varphi(m)$ – функция Эйлера, равная числу чисел в ряду от 0 до $m-1$, взаимно простых с m.

Функция Эйлера может быть вычислена следующим образом:

$$\phi(m) = \prod_{i=1}^{t} p_i^{l_i - 1}(p_i - 1),$$

причем m представляется как составное число в виде

$$m = \prod_{i=1}^{t} p_i^{l_i},$$

где $p_i > 1$ – простое; l_i – натуральное число; $i = 1,2,...,t$.

Число примитивных элементов в поле GF(p^n) равно

$$N_{\varepsilon_{max}} = \phi(p^n - 1).$$

Далее, если α – примитивный элемент поля GF(p^n), то мультипликативно обратный элемент α^{-1} также является примитивным, так как

$$-1 \equiv p^n - 2 \pmod{p^n - 1},$$

а числа $p^n - 1$ и $p^n - 2$ всегда взаимно просты.

Можно показать, что свойство равенства периодов прямых и мультипликативно обратных элементов выполняется не только для примитивных, но и для элементов с произвольным периодом ε.

Понятие периода элемента является одним из ключевых в теории конечных полей. В частности, оно используется при доказательстве знаменитой теоремы Ферма о структуре конечного поля.

Теорема Ферма. Любой элемент поля GF(p^n) удовлетворяет сравнению

$$x^{p^n} - x \equiv 0.$$

Следствием теоремы Ферма является тот факт, что полином в левой части сравнения может быть представлен в виде произведения p^n сомножителей следующим образом:

$$x^{p^n} - x = \prod_{i=1}^{p^n} (x - a_i),$$

где $a_i \in$ GF(p^n) – все различные элементы поля.

Данное выражение показывает, что все элементы поля GF(p^n) являются корнями полинома $x^{p^n} - x$, причем каждый корень встречается только один раз.

При построении мультипликативной группы поля GF(p^n) примитивный элемент α, имеющий максимальный период $\varepsilon_{max} = p^n - 1$, выступает в роли образующего элемента. Если ε_{max} – составное число, то существуют элементы поля с периодами $1 < \varepsilon < p^n - 1$, которые являются делителями ε_{max}. Каждый элемент с

периодом ε является образующим элементом группы порядка ε, которая называется подгруппой мультипликативной группы поля.

2.5 Минимальные полиномы

В соответствии с теоремой Ферма о конечном поле GF(p^n) любой элемент этого поля является корнем уравнения

$$x^{p^n} - x = 0,$$

что позволяет представить данный полином в виде произведения сомножителей:

$$x^{p^n} - x = \prod_{i=0}^{p^n-1}(x - a_i),$$

где a_i пробегают все элементы поля.

Определение. *P*–сопряженными элементами для элемента $a \in$ GF(p^n) называются элементы, удовлетворяющие выражению

$$a^{p^i},\ i = 0,1,2,...$$

При этом число k различных p-сопряженных элементов называется степенью элемента a.

Определение. Минимальным полиномом $m_a(x)$ для элемента $a \in$ GF(p^n) называется полином минимальной степени, корнями которого являются элемент a и его различные p–сопряженные элементы:

$$m_a(x) = \prod_{i=0}^{k-1}(x - a^{p^i}).$$

Степень k минимального полинома равна числу различных p–сопряженных элементов для элемента a. Таким образом, p-сопряженные элементы имеют один и тот же минимальный полином.

В поле GF(p^n) минимальный полином $m_a(x)$ имеет ровно k корней. В то же время над полем GF(p) он является неприводимым, т.е. неразложимым на множители с коэффициентами из GF(p).

Методика вычисления минимальных полиномов:

1. Построение поля GF(p^n) для заданных неприводимого полинома $f(x)$ и примитивного элемента α.

2. Определение p-сопряженных элементов для заданных элементов поля, определение чисел k, равных степеням минимальных полиномов.

3. Вычисление минимальных полиномов в соответствии с *Определение*м.

В общем случае полином $x^{p^n} - x$ равен произведению различных минимальных полиномов.

Для произвольного полинома над полем GF(p^n) всегда существует полином, корнями которого являются элементы поля, мультипликативно обратные корням данного полинома. Такие полиномы называются сопряженными.

Определение. Пусть корнями полинома $f(x)$ являются p-сопряженные элементы для элемента α^j, тогда полином $f^*(x)$, корнями которого будут мультипликативно обратный элемент α^{-j} и его p-сопряженные элементы, называется

сопряженным полиномом. Вычисление сопряженного полинома $f^*(x)$ по исходному полиному $f(x)$ степени r производится в соответствии с выражением

$$\begin{cases} f(x) = x^r + f_{r-1}x^{r-1} + ... + f_1 x + f_0, \\ f^*(x) = x^r f_0^{-1} f(x^{-1}), \end{cases}$$

где $f(x^{-1})$ – полином с аддитивно обратными показателями степеней переменной x полинома $f(x)$; f_0^{-1} – элемент, мультипликативно обратный коэффициенту при нулевой степени переменной x полинома $f(x)$, данный множитель вводится для обеспечения условия нормировки полинома $f^*(x)$.

2.6 Простейшие функции в конечных полях

2.6.1 Функция следа элементов поля

Во многих практических приложениях сумма корней минимальных полиномов выступает в виде самостоятельного математического объекта. Это определило необходимость введения специальной функции для произвольного элемента поля, которая получила название функции следа.

Определение. Пусть GF(p^n) – расширение степени n простого поля GF(p). Функцией следа (следом) $\mathrm{tr}_{n1}a$ элемента a поля GF(p^n) в простом поле GF(p) называется сумма вида

$$\mathrm{tr}_{n1}a = \sum_{i=0}^{n-1} a^{p^i} = a + a^p + a^{p^2} + ... + a^{p^{n-1}}.$$

Напомним, что элементы a^{p^i} (i = 0,1,...) называются p–сопряженными элементами. Если один из них является корнем минимального полинома степени n, то и остальные элементы являются корнями этого полинома. При p = 2 множество {i, 2i, 4i,...} показателей степени p-сопряженных элементов называется циклотомическим классом. При произвольном p циклотомический класс определяется выражением {ip, ip^2, ..., ip^j,...}.

Свойства функции следа:

1) функция следа есть отображение расширенного поля GF(p^n) в простое поле GF(p):

$$\mathrm{tr}_{n1}a \in \mathrm{GF}(p), \forall a \in \mathrm{GF}(p^n);$$

2) $(\mathrm{tr}_{n1}a)^{p^m} = \mathrm{tr}_{n1}a^{p^m}$, где p – характеристика поля, m – целое;

3) функция следа – линейное отображение GF(p^n) $\rightarrow$ GF(p);

4) когда a пробегает все элементы поля GF(p^n), $\mathrm{tr}_{n1}a$ принимает каждое из значений в GF(p) ровно p^{n-1} раз.

Очевидно, что все p-сопряженные элементы имеют одинаковые следы.

2.6.2 Аддитивный и мультипликативный характеры

Использование теории конечных групп и полей при синтезе кодовых последовательностей предполагает введение некоторого отображения, связывающего элементы конечных полей с символами кодовых последовательностей,

являющихся комплексными либо действительными числами. В качестве таких соответствий широкое распространение получили характеры аддитивной и мультипликативной групп поля GF(p^n), т. е. отображения названных групп на группу $\tilde{G}_M$ комплексных корней из единицы степени M, где M – порядок (число элементов) группы $\tilde{G}_M$.

Пусть GF(p^n) – поле характеристики p, а $\mathrm{tr}_{n1}\alpha$ – след элемента $\alpha \in$ GF(p^n) в простом подполе GF(p), т. е. $\mathrm{tr}_{n1}\alpha$ может принимать значения от 0 до p–1. Введение функции $\exp(j2\pi \mathrm{tr}_{n1}\alpha/p)$, в которой вычисление экспоненты понимается как обычные действия с комплексными числами, позволяет дать следующее *Определение* аддитивному характеру.

Определение. Характером аддитивной группы $G_+(p^n)$ поля GF(p^n) (аддитивным характером) называется отображение конечного поля GF(p^n) в группу комплексных чисел $\tilde{G}_p$

$$e(x) = \exp(j2\pi \mathrm{tr}\mu x/p),\ x \in \mathrm{GF}(p^n),$$

которое удовлетворяет соотношению $e(x+y) = e(x)\cdot e(y)$ при любом фиксированном $\mu \in$ GF(p^n).

Таким образом, аддитивный характер поля GF(p^n) может принимать ровно p комплексных значений. Для полей характеристики $p = 2$ эти значения соответственно равны 1 и –1. Так как порядки поля и его аддитивной группы совпадают, то термины «характер аддитивной группы поля» и «аддитивный характер поля» считаются эквивалентными.

Для определения мультипликативного характера обозначим через $\log_\alpha\beta$ показатель степени k в равенстве $\beta = \alpha^k$, где α – примитивный элемент поля GF(p^n).

Определение. M-значным характером мультипликативной группы $G_\times$ поля GF(p^n) (M-значным мультипликативным характером) называется отображение группы $G_\times$ в группу комплексных чисел $\tilde{G}_M$:

$$\psi(x) = \exp(j2\pi \log_\alpha x/M),\ x \in G_\times,$$

которое удовлетворяет соотношению $\psi(xy) = \psi(x)\psi(y),\ \forall\ x,y \in G_\times$ при значениях M, являющихся делителями порядка мультипликативной группы $L = p^n$–1.

Таким образом, в аддитивном характере $e(x)$ в показатель экспоненты входит след элемента расширенного поля $\mathrm{tr}_{n1}\alpha$ и характеристика поля p. В мультипликативном характере $\psi(x)$ – степень k примитивного элемента α^k и делитель M порядка мультипликативной группы.

В частном, но широко распространенном в настоящее время случае передачи двоичных сигналов характеры $e(x)$ и $\psi(x)$ используются для перехода от алфавита {0,1} к алфавиту {1, –1}.

2.6.3 Производная в конечном поле

В практических приложениях теории конечных полей, например при реализации алгебраического метода декодирования помехоустойчивых цикличе-

ских кодов, встречается понятие производной по переменной x полинома $A(x)$, построенного над конечным полем:

$$A(x) = \sum_{i=0}^{m} a_i x^i = a_0 + a_1 x + ... + a_m x^m ,$$

где $\alpha_i \in \mathrm{GF}(p^n)$ – элементы расширенного поля.

Для полей характеристики $p = 2$ можно дать следующее *Определение* производной функции над конечным полем.

Определение. Производной функцией по переменной x полинома $A(x)$ называется функция $A'_x(x)$, определяемая выражением

$$A'_x(x) = \sum_{i=0}^{j} a_{2i+1} x^{2i} = a_1 + a_3 x^2 + a_5 x^4 + ... + a_{2j+1} x^{2j} ,$$

где $j = \lfloor (m-1)/2 \rfloor$ – целая часть числа.

При вычислении производной в полях характеристики $p > 2$ в нуль обращаются только те слагаемые полинома, степень переменной x которых кратна p. С остальными показателями проводится операция по модулю p.

При вычислении производных более высоких порядков необходимо учитывать, что они равны нулю, начиная с p-й производной.

Для производной над конечным полем справедливы свойства обычной производной для суммы и произведения двух функций.

2.7 Задачи

Задача 2.1. В поле $GF(7)$ для элементов 2, 3, 5 определить обратные по сложению элементы.

Задача 2.2. В поле $GF(7)$ для элементов 2, 3, 5, 6 найти обратные по умножению элементы.

Задача 2.3. Вычислить мультипликативно обратные элементы и найти их сумму S по модулю m =7:

а) S = [(3–1 mod 7)+(5–1 mod 11)+(3–1 mod 5)+(4–1 mod 13)] mod 7;

б) S = [(2–1 mod 7)+(7–1 mod 11)+(4–1 mod 5)+(5–1 mod 13)] mod 7;

в) S = [(4–1 mod 7)+(6–1 mod 11)+(4–1 mod 5)+(5–1 mod 13)] mod 7;

г) S = [(5–1 mod 7)+(8–1 mod 11)+(2–1 mod 3)+(3–1 mod 13)] mod 7.

Задача 2.4. Построить таблицы сложения и умножения для простых полей:

а) $GF(2)$ с элементами 0, 1;

б) $GF(3)$ с элементами 0, 1, 2.

Задача 2.5. Построить таблицы вычитания для аддитивных групп:

а) $G_+ = \{0,1\}$, $m = 2$;

б) $G_+ = \{0,1,2\}$, $m = 3$;

в) $G_+ = \{0,1,2,3\}$, $m = 4$.

Задача 2.6. Составить таблицы сложения, вычитания и умножения элементов полей:

а) $GF(5)$;

б) $GF(7)$;

в) $GF(6)$.

Задача 2.7. Вычислить:

а) x^5+x^4+x+1 modd $(x^3+x+1, 2)$;

б) $x^6-3x^5+2x^4-1$ modd $(x^3+4x^2+2, 5)$;

в) $x^5+2x^4-2x^2+x$ modd $(x^2-x-2, 3)$;

г) $x^5-3x^4-6x^3+5$ modd $(x^3-6x^2+4, 7)$.

Задача 2.8. Пусть $F(x) = x^3+x+1$, $p = 2$ и заданы полиномы $A_1(x) = x^5+x^3+x+1$, $A_2(x) = x^4+x^3+x^2+1$. Определить $B_1(x)$, $B_2(x)$.

Задача 2.9. Пусть $F(x) = x^3+4x^2+2x+3$, $p = 5$, $A(x) = x^6-x^5-4x-2$. Определить $B(x)$.

Задача 2.10. Определить элементы расширенного поля $GF(2^2)$ и построить таблицы сложения и умножения элементов поля (таблицы Кэли).

Задача 2.11. Построить таблицы сложения и умножения элементов множества F как полной системы полиномов – вычетов вида

$$R(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + ... + a_1x + a_0,$$

(где $a_i \in GF(p)$, $i = \overline{0, n-1}$ – элементы простого поля) по модулю полинома $f(x) = x^3+x^2+x+1$, являющегося приводимым полиномом степени $n = 3$ над полем $GF(2)$, т.е. $f(x) = (x^2+1)(x+1)$. Определить, является ли множество F полем Галуа.

Задача 2.12. Определить элементы расширенного поля $GF(3^2)$ с неприводимым полиномом $f(x) = x^2+2x+2$ и построить таблицы сложения и умножения.

Задача 2.13. Построить расширенное поле $GF(2^3)$ с неприводимым полиномом $f(x) = x^3+x+1$, если в качестве примитивного элемента использовать $\alpha = a$.

Задача 2.14. Построить расширенное поле $GF(3^2)$ с неприводимым полиномом $f(x) = x^2+x+2$ и примитивным элементом $\alpha = a$.

Задача 2.15. Построить расширенное поле $GF(2^3)$ с неприводимым полиномом $f(x) = x^3+x^2+1$ и примитивным элементом $\alpha = a$.

Задача 2.16. Задано поле $GF(2^3)$, $f(x) = x^3+x+1$, $\alpha = a$. Упростить выражение и найти его значение в точке $x = 5$: $A(x) = (7x^4+4x^3+x+2)(3x+4)$.

Задача 2.17. Для поля $GF(2^3)$, $f(x) = x^3+x^2+1$, $\alpha = a$ упростить выражения и найти их значения в точке $x = 7$: $A(x) = (3x^2+2)(4x+1)(6x+7)$;
$B(x) = (5x^2+4x^3+2x^2+x+7)(x^2+4)$.

Задача 2.18. Задано поле $GF(2^3)$, $f(x) = x^3+x+1$, $\alpha = a$. Упростить выражение и найти его значение в точке $x = 5$: $A(x) = (7x^4+4x^3+x+2)(3x+4)$.

Задача 2.19. Задано поле Галуа $GF(2^6)$, $f(x) = x^6+x+1$, $\alpha = a$, $\varepsilon(\alpha) = 63$. Определить периоды элементов.

Задача 2.20. Построить расширенное поле $GF(2^4)$, $f(x)=x^4+x+1$, $\alpha = a$ (показать степенное и полиномиальное представление элементов). Определить число k различных p-сопряженных элементов для элементов α^4 и α^6. Определить минимальные полиномы для элементов α^2 и α^5.

Задача 2.21. Построить расширенное поле $GF(3^2)$, $f(x) = x^2+x+2$, $\alpha = a$ (показать степенное и полиномиальное представление элементов). Определить число k различных p-сопряженных элементов для элементов α^4 и α^6. Определить минимальные полиномы для элементов α^2 и α^5.

Задача 2.22. Построить основное расширенное поле $GF(3^2)$, $\pi(x)$, $\alpha = a$ и автоморфное поле для $\beta = \alpha^i$. Определить функцию следа, минимальный полином, аддитивный характер и четырехзначный ($M = 4$) мультипликативный характер для элемента β^j, если $\mu = 1$.

а) $\pi(x)= x^2+x+2$; $i=3$; $j=5$;

б) $\pi(x)= x^2+2x+2$; $i=3$; $j=5$;

в) $\pi(x)= x^2+x+2$; $i=5$; $j=7$;

г) $\pi(x)= x^2+2x+2$; $i=5$; $j=7$;

д) $\pi(x)= x^2+x+2$; $i=7$; $j=3$;

е) $\pi(x)= x^2+2x+2$; $i=7$; $j=3$.

Задача 2.23. Задано поле $GF(2^4)$, $f(x) = x^4+x^3+x^2+x+1$. Проверить элементы $\alpha = a$, a^3+a^2 и $a+1$ на примитивность, построить поле, определить периоды, функции следа и минимальные полиномы для его элементов.

Задача 2.24. Задано поле Галуа $GF(2^4)$, $f(x) = x^4+x+1$, $\alpha = a$, $\varepsilon(\alpha) = p^n-1$. Определить периоды элементов α^3, α^5, α^7, α^{14}.

Задача 2.25. Задано поле Галуа $GF(2^6)$, $f(x) = x^6+x+1$, $\alpha = a$, $\varepsilon(\alpha) = 63$. Определить периоды элементов α^4, α^{27}, α^{42}, α^{49}, α^{57}, α^0.

Задача 2.26. Задано поле Галуа $GF(2^6)$. Определить число элементов с периодами 1, 3, 7, 9, 21, 63.

Задача 2.27. Показать, что элементы поля $GF(2^4)$, мультипликативно обратные примитивным элементам α, α^4, α^7, α^{13}, являются примитивными.

Задача 2.28. Построить поле $GF(2^2)$, $f(x) = x^2+x+1$, $\alpha = a$. Проверить выполнение теоремы Ферма и выражения (2.18).

Задача 2.29. Определить все подгруппы мультипликативной группы поля $GF(2^4)$, $f(x) = x^4+x+1$, $\alpha = a$.

Задача 2.30. Разложить мультипликативную группу G поля $GF(2^4)$, $f(x) = x^4+x+1$, $\alpha = a$ на непересекающиеся смежные классы по подгруппе $H = \{1,\alpha^3,\alpha^6,\alpha^9,\alpha^{12}\}$.

Задача 2.31. Определить все различные подполя конечного поля $GF(2^{18})$.

Задача 2.32. Определить все различные подполя конечного поля $GF(2^{18})$.

Задача 2.33. Определить число k различных p-сопряженных элементов для элементов α, α^3, α^4, α^6, α^5, α^0 конечных полей $GF(2^3)$, $GF(3^2)$ и $GF(2^4)$.

Задача 2.34. Определить минимальные полиномы для элементов поля $GF(2^3)$, $f(x) = x^3+x+1$, $\alpha = a$.

Задача 2.35. Определить минимальные полиномы для элементов поля $GF(3^2)$, $f(x) = x^2+x+2$, $\alpha = a$.

Задача 2.36. Определить сопряженные полиномы для полиномов $f_1(x) = x^4+x+1$, $f_2(x) = x^4+x^3+ +x^2+x+1$ над полем $GF(2^4)$, $f(x) = x^4+x+1$, $\alpha = a$ и для полиномов $f_3(x) = x^2+2x+2$, $f_4(x) = x^2+1$, $f_5(x) = x+2$ над полем $GF(3^2)$, $f(x) = = x^2+x+2$, $\alpha = a$.

Задача 2.37. Построить поле $GF[(2^2)^2]$, $f_s(z) = z^2+z+a$, $f_n(a) = a^2+a+1$, $\alpha = x$, определить периоды элементов и их минимальные полиномы.

Умножение в поле $GF(2^2)$ $f_n(a) = a^2+a+1$

⊗	0	1	a	a+1
0	0	0	0	0
1	0	1	a	a+1
a	0	a	a+1	1
a+1	0	a+1	1	a

Задача 2.38. Задано поле $GF(2^3)$, $f(x) = x^3+x+1$, $\alpha = a$ (см. решение задачи 2.7). Определить функцию следа для элементов α^0, α, α^3, α^4.

Задача 2.39. Определить функции следа для элементов поля $GF[(2^2)^2]$, $f_s(z) = z+z+a$, $f_n(a) = a^2+a+1$, $\alpha = a$ в простом поле $GF(2)$ и в расширенном поле $GF(2^2)$.

Задача 2.40. Определить аддитивные характеры элементов $x = \alpha$, α^4, α^7 поля $GF(3^2)$, $f(x) = x^2+x+2$, $\alpha = a$, построенного в задаче 2.20, для $\mu = \alpha^5$.

Задача 2.41. Определить мультипликативные характеры для элементов $x = \alpha^0$, α, α^4, α^7 поля $GF(3^2)$, $f(x) = x^2+x+2$, $\alpha = a$, построенного в задаче 2.20, для $M_1 = 2$, $M_2 = 4$.

Задача 2.42. Над полем $GF(2^4)$ определить производные функции для следующих полиномов $A_1(x) = x^{12}+\alpha^3x^{11}+\alpha^8x^7+\alpha^5x^4+\alpha x^2+\alpha^8$, $A_2(x)=3x^{11}+8x^{10}+4x^5+6x^3+2x^2+7$.

Задача 2.43. Над полем $GF(5^2)$ определить производную функцию для полинома $A(x) = \alpha^5x^{14}+ +4\alpha^{17}x^{12}+3\alpha^{23}x^{10}+\alpha x^8+2\alpha^5x^7+4\alpha x^5+3x+4\alpha^2$.

2.8 Решения

Решение к задаче 2.1.

Сумма обратных по сложению элементов равна нейтральному элементу, т.е. 0 mod 7.

Для элемента 2: $2+x=0 \Rightarrow x= 5$.

Для элемента 3: $3+x=0 \Rightarrow x= 4$.

Для элемента 5: $5+x=0 \Rightarrow x= 2$.

Ответ: обратные по сложению элементы для 2 – 5, для 3 – 4, для 5 – 2.

Решение к задаче 2.2.

Произведение обратных по умножению элементов равно нейтральному элементу, т.е. 1 mod 7.

Для элемента 2: $2\cdot x = 1 \bmod 7 \Rightarrow x= 4$.

Для элемента 3: $3\cdot x = 1 \bmod 7 \Rightarrow x= 5$.

Для элемента 5: $5\cdot x = 1 \bmod 7 \Rightarrow x= 3$.

Для элемента 6: $6\cdot x = 1 \bmod 7 \Rightarrow x= 6$.

Ответ: обратные по умножению элементы для 2 – 4, для 3 – 5, для 5 – 3, для 6 – 6.

Решение к задаче 2.3.

а) $S = [(3–1 \bmod 7)+(5–1 \bmod 11)+(3–1 \bmod 5)+(4–1 \bmod 13)] \bmod 7 =$
$= (5+9+2+10) \bmod 7 = 5$;

б) S = [(2–1 mod 7)+(7–1 mod 11)+(4–1 mod 5)+(5–1 mod 13)] mod 7 = = (4+8+4+8) mod 7 = 3;

в) S = [(4–1 mod 7)+(6–1 mod 11)+(4–1 mod 5)+(5–1 mod 13)] mod 7 = = (2+2+4+8) mod 7 = 2;

г) S = [(5–1 mod 7)+(8–1 mod 11)+(2–1 mod 3)+(3–1 mod 13)] mod 7 = = (3+7+2+9) mod 7 = 0.

Решение к задаче 2.4.

а) *GF*(2) с элементами 0, 1

$m = p = 2$

⊕	0	1
0	0	1
1	1	0

⊗	0	1
0	0	0
1	0	1

б) *GF*(3) с элементами 0, 1, 2

$m = p = 3$

⊕	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

⊗	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Решение к задаче 2.5.

а) $G_+ = \{0,1\}$, $m = 2$; б) $G_+ = \{0,1,2\}$, $m = 3$; в) $G_+ = \{0,1,2,3\}$, $m = 4$.

⊖	0	1
0	0	1
1	1	0

⊖	0	1	2
0	0	2	1
1	1	0	2
2	2	1	0

⊖	0	1	2	3
0	0	3	2	1
1	1	0	3	2
2	2	1	0	3
3	3	2	1	0

Решение к задаче 2.6.

а) *GF*(5):

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

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

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

б) *GF*(7):

⊕	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

⊗	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2		4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

⊖	0	1	2	3	4	5	6
0	0	6	5	4	3	2	1
1	1	0	6	5	4	3	2
2	2	1	0	6	5	4	3
3	3	2	1	0	6	5	4
4	4	3	2	1	0	6	5
5	5	4	3	2	1	0	6
6	6	5	4	3	2	1	0

в) $GF(6)$:

$\oplus$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	4	3	2	1	0

$\otimes$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

$\ominus$	0	1	2	3	4	5
0	0	5	4	3	2	1
1	1	0	5	4	3	2
2	2	1	0	5	4	3
3	3	2	1	0	5	4
4	4	3	2	1	0	5
5	5	4	3	2	1	0

Решение к задаче 2.7.

а) $x^5+x^4+x+1 \bmod(x^3+x+1, 2)$.

$$\begin{array}{l|l} x^5+x^4+x+1 & x^3+x+1 \\ \ominus\ x^5+x^3+x^2 & \hline x^2+x+1 \\ \hline x^4+x^3+x^2+x+1 & \\ \ominus\ x^4+x^2+x & \\ \hline x^3+1 & \\ \ominus\ x^3+x+1 & \\ \hline x & \end{array}$$

б) $x^6-3x^5+2x^4-1 \bmod(x^3+4x^2+2, 5)$.

$$\begin{array}{l|l} x^6-3x^5+2x^4-1 & x^3+4x^2+2 \\ \ominus\ x^6+4x^5+2x^3 & \hline x^3+3x^2+3 \\ \hline 3x^5+2x^4+3x^3+4 & \\ \ominus\ 3x^5+2x^4+x^2 & \\ \hline 3x^3+4x^2+4 & \\ \ominus\ 3x^3+2x^2+1 & \\ \hline 2x^2+3 & \end{array}$$

Проверка:

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

$= 2x^2+3+x^6+3x^5+3x^3+4x^5+2x^4+2x^2+2x^3+x^2+1 = x^6+2x^5+2x^4+4.$

в) $x^5+2x^4-2x^2+x \bmod(x^2-x-2, 3)$.

$$\begin{array}{l|l} x^5+2x^4-2x^2+x & x^2-x-2 \\ \ominus\ x^5-x^4-2x^3 & \hline x^3+3x^2+3 \\ \hline 2x^3-2x^2+x & \\ \ominus\ 2x^3-2x^2-x & \\ \hline 2x & \end{array}$$

Проверка:

$x^5+2x^4-2x^2+x = 2x+(x^2-x-2)\cdot(x^3+3x^2+3) = 2x+x^5+2x^3-x^4-2x^2-2x^3-x =$

$= x^5-x^4-2x^2+x.$

г) $x^5-3x^4-6x^3+5 \bmod(x^3-6x^2+4, 7)$.

$$\begin{array}{l|l} x^5-3x^4-6x^3+5 & x^3-6x^2+4 \\ \ominus\ x^5-6x^4+4x^2 & \hline x^2+3x+5 \end{array}$$

$$\begin{array}{l} \overline{3x^4-6x^3-4x^2+5} \\ \ominus\ \underline{3x^4+3x^3+5x} \\ \overline{5x^3-4x^2-5x+5} \\ \ominus\ \underline{5x^3-2x^2+6} \\ \overline{5x^2-5x-1} \end{array}$$

Проверка:

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

$= 5x^2-5x-1+x^5-6x^4+4x^2+3x^4-4x^3+5x+5x^3-2x^2+6 = x^5-3x^4+x^3+5$

Решение к задаче 2.8.

$B(x) \equiv A(x)$ modd$(F(x),p)$.

1) $x^5+x^3+x+1 \equiv (x^2+x+1)$ modd$(x^3+x+1, 2)$, так как

$$\begin{array}{l|l} x^5+x^3+x+1 & x^3+x+1 \\ \ominus\ \underline{x^5+x^3+x^2\ \ \ } & \overline{x^2=K(x)} \\ x^2+x+1 = R_1(x) & \end{array}$$

$B_1(x) = R_1(x) = x^2+x+1$.

2) $x^4+x^3+x^2+1 \equiv 0$ modd$(x^3+x+1,2)$, так как

$$\begin{array}{l|l} x^4+x^3+x^2+1 & x^3+x+1 \\ \ominus\ \underline{x^4+x^2+x\ \ \ } & \overline{x+1=K(x)} \\ x^3+x+1 & \\ \ominus\ \underline{x^3+x+1\ \ \ } & \\ 0 = R_2(x); & \end{array}$$

$B_2(x) = R_2(x) = 0$

Решение к задаче 2.9.

$B(x) \equiv A(x)$ modd$(F(x),p) \equiv (x^6+4x^5+x+3)$ modd$(x^3+4x^2+2x+3,5)$.

$$\begin{array}{l|l} x^6+4x^5+x+3\ \ \ & x^3+4x^2+2x+3 \\ \ominus\ \underline{x^6+4x^5+2x^4+3x^3} & \overline{x^3+3x=K(x)} \\ 3x^4+2x^3+x+3 & \\ \ominus\ \underline{3x^4+2x^3+x^2+4x\ \ \ } & \\ 4x^2+2x+3 = R(x) & \end{array}$$

$B(x) = R(x) = 4x^2+2x+3$.

Проверка правильности вычисления $B(x)$:

$A(x) = B(x)+K(x)F(x) = 4x^2+2x+3+(x^3+3x)(x^3+4x^2+2x+3)=x^6+4x^5+x+3$.

Решение к задаче 2.10.

1) Число элементов поля (порядок поля) равно $L = p^n = 2^2=4$.

2) Полагая $n = 2$ и придавая коэффициентам a_i независимо значения элементов поля $GF(2)$ (т.е. числа 0 и 1), получаем $GF(2^2) = \{0, 1, x, x+1\}$.

Элементами расширенного поля $GF(2^2)$ являются полиномы степени не выше $n-1$ с коэффициентами из $GF(2)$.

3) При построении таблицы сложения учитывается, что операция выполняется по mod 2.

$\oplus$	0	1	x	x+1
0	0	1	x	x+1
1	1	0	x+1	x
x	x	x+1	0	1
x+1	x+1	x	1	0

4) При составлении таблицы умножения элементов поля $GF(2^2)$ требуется конкретизация неприводимого полинома $f(x)$, так как умножение элементов осуществляется по двойному модулю ($f(x)$, p). Для расширенного поля $GF(2^2)$ существует единственный неприводимый над $GF(2)$ полином степени 2 – $f(x) = x^2+x+1$ (неприводимость $f(x)$ легко проверить, попытавшись разделить его на полиномы x и x+1 без остатка).

Определим, к примеру, произведение элементов x+1 и x+1. Выполняя умножение, получаем

$$(x+1)(x+1) = x^2+1 (\mathrm{mod}\ 2).$$

Разделив полином x^2+1 на полином x^2+x+1, находим

$$\begin{array}{l|l} x^2+1 & x^2+x+1 \\ \ominus\ \underline{x^2+x+1} & 1 \\ x & \end{array}$$

Следовательно, $(x+1)(x+1) \equiv x\ \mathrm{modd}(x^2+x+1, 2)$.

Аналогичным образом определяются произведения всех возможных пар элементов поля $GF(2^2)$.

$\otimes$	0	1	x	x+1
0	0	0	0	0
1	0	1	x	x+1
x	0	x	x+1	1
x+1	0	x+1	1	x

Решение к задаче 2.11.

1) Элементы множества F образуют полную систему полиномов – вычетов по двойному модулю ($f(x)$, p = 2):

$F = \{0, 1, x, x+1, x^2, x^2+1, x^2+x+1, x^2+x\}$.

2) Построим таблицы сложения и умножения.

$\oplus$	0	1	x	x^2	x+1	x^2+1	x^2+x	x^2+x+1
0	0	1	x	x^2	x+1	x^2+1	x^2+x	x^2+x+1
1	1	0	x+1	x^2+1	x	x^2	x^2+x+1	x^2+x
x	x	x+1	0	x^2+x	1	x^2+x+1	x^2	x^2+1
x^2	x^2	x^2+1	x^2+x	0	x^2+x+1	1	x	x+1
x+1	x+1	x	1	x^2+x+1	0	x^2+x	x^2+1	x^2
x^2+1	x^2+1	x^2	x^2+x+1	1	x^2+x	0	x+1	x
x^2+x	x^2+x	x^2+x+1	x^2	x	x^2+1	x+1	0	1
x^2+x+1	x^2+x+1	x^2+x	x^2+1	x+1	x^2	x	1	0

№ строки	⊗	1	x	x^2	$x+1$	x^2+1	x^2+x	x^2+x+1
1	1	1	x	x^2	$x+1$	x^2+1	x^2+x	x^2+x+1
2	x	x	x^2	x^2+x+1	x^2+x	x^2+1	$x+1$	1
3	x^2	x^2	x^2+x+1	1	$x+1$	x^2+1	x^2+x	x
4	$x+1$	$x+1$	x^2+x	$x+1$	x^2+1	0	x^2+1	x^2+x
5	x^2+1	x^2+1	x^2+1	x^2+1	0	0	0	x^2+1
6	x^2+x	x^2+x	$x+1$	x^2+x	x^2+1	0	x^2+1	$x+1$
7	x^2+x+1	x^2+x+1	1	x	x^2+x	x^2+1	$x+1$	x^2

Для примера определим произведение элементов (x^2+x) и (x^2+x+1). Выполняя умножение, получим

$$(x^2+x)(x^2+x+1) = (x^4+x^3+x^3+x^2+x^2+x) \bmod 2 = x^4+x.$$

Найдем остаток от деления полинома (x^4+x) на $f(x) = x^3+x^2+x+1$:

$$\begin{array}{l|l} x^4+x & x^3+x^2+x+1 \\ \ominus\ \underline{x^4+x^3+x^2+x} & x+1 \\ \quad x^3+x^2 & \\ \ominus\ \underline{x^3+x^2+x+1} & \\ \qquad\quad x+1 & \end{array}$$

Следовательно, $(x^2+x)(x^2+x+1) = x+1$ modd $(x^3+x^2+x+1, 2)$. Аналогичным образом вычисляются остальные произведения.

3) Множество F не является полем, так как для элементов $x+1$, x^2+1 и x^2+x не существует мультипликативно обратных элементов, что определяется отсутствием единичного элемента в 4, 5 и 6 строках таблицы умножения.

Решение к задаче 2.12.

1) Элементы расширенного поля $GF(3^2)$ образуют полную систему полиномов – вычетов по двойному модулю ($f(x)$, $p = 3$):

$GF(3^2) = \{0, 1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2\}$.

2) Построим таблицы сложения и умножения.

⊕	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
0	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
1	1	2	0	$x+1$	$x+2$	x	$2x+1$	$2x+2$	$2x$
2	2	0	1	$x+2$	x	$x+1$	$2x+2$	$2x$	$2x+1$
x	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$	0	1	2
$x+1$	$x+1$	$x+2$	x	$2x+1$	$2x+2$	$2x$	1	2	0
$x+2$	$x+2$	x	$x+1$	$2x+2$	$2x$	$2x+1$	2	0	1
$2x$	$2x$	$2x+1$	$2x+2$	0	1	2	x	$x+1$	$x+2$
$2x+1$	$2x+1$	$2x+2$	$2x$	1	2	0	$x+1$	$x+2$	x
$2x+2$	$2x+2$	$2x$	$2x+1$	2	0	1	$x+2$	x	$x+1$

⊗	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
1	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
2	2	1	$2x$	$2x+2$	$2x+1$	x	$x+2$	$x+1$
x	x	$2x$	$x+1$	$2x+1$	1	$2x+2$	2	$x+2$

$\otimes$	1	2	x	x+1	x+2	2x	2x+1	2x+2
x+1	x+1	2x+2	2x+1	2	x	x+2	2x	1
x+2	x+2	2x+1	1	x	2x+2	2	x+1	2x
2x	2x	x	2x+2	x+2	2	x+1	1	2x+1
2x+1	2x+1	x+2	2	2x	x+1	1	2x+2	x
2x+2	2x+2	x+1	x+2	1	2x	2x+1	x	2

Для примера определим произведение элементов (2x+2) и (2x+1). Выполняя умножение, получим

$$(2x+2)(2x+1) = (4x^2+2x+4x+2) \bmod 3 = x^2+2.$$

Найдем остаток от деления полинома (x^2+2) на $f(x) = x^2+2x+2$, при этом все вычисления будем производить по модулю 3:

$$\begin{array}{r|l} x^2+2 & x^2+2x+2 \\ \ominus\ \underline{x^2+2x+2} & 1 \\ x & \end{array}$$

Следовательно, (2x+2)(2x+1) = x modd(x^2+2x+2, 3). Аналогичным образом вычисляются остальные произведения.

Решение к задаче 2.13.

1) Проведем последовательное возведение в степень элемента $\alpha = a$ с учетом того, что операции выполняются по двойному модулю ($f(a)$, 2):

$\alpha^0 = 1$;

$\alpha^1 = a$;

$\alpha^2 = a^2$;

$\alpha^3 = a^3 \bmod f(a) = a + 1$;

$\alpha^4 = a^2 + a$;

$\alpha^5 = (a^3 + a^2) \bmod f(a) = a^2 + a + 1$;

$\alpha^6 = (a^3 + a^2 + a) \bmod f(a) = (a + 1 + a^2 + a) \bmod 2 = a^2 + 1$;

$\alpha^7 = (a^3 + a) \bmod f(a) = (a + 1 + a) \bmod 2 = 1$.

Для обозначения нулевого элемента поля используется формальная запись $\alpha^{-\infty} = 0$.

2) Очевидно, что период элемента a равен $\varepsilon(a)=7$, т.е. равен $\varepsilon_{max}=2^3-1$ – порядку мультипликативной группы поля. Свойство цикличности группы проявляется в том, что $\alpha^7 = \alpha^0 = 1$, $\alpha^8 = \alpha^1$, $\alpha^9 = \alpha^2$ и т.д.

Целочисленная	Степенная	Полиномиальная	Векторная
0	$\alpha^{-\infty}$	0	0 0 0
1	α^0	1	0 0 1
2	α^1	a	0 1 0
3	α^2	a^2	1 0 0
4	α^3	a+1	0 1 1
5	α^4	a^2+a	1 1 0
6	α^5	a^2+a+1	1 1 1
7	α^6	a^2+1	1 0 1

Решение к задаче 2.14.

Для обозначения нулевого элемента поля используется формальная запись $\alpha^{-\infty} = 0$.

Проведем последовательное возведение в степень элемента $\alpha = a$ с учетом того, что операции выполняются по двойному модулю ($f(a)$, 3):

Целочисленная	Степенная	Полиномиальная	Векторная
0	$\alpha^{-\infty}$	0	00
1	α^0	1	01
2	α^1	a	10
3	α^2	2a+1	21
4	α^3	2a+2	22
5	α^4	2	02
6	α^5	2a	20
7	α^6	a+2	12
8	α^7	a+1	11

Полиномиальное представление элементов поля вычисляется последовательным возведением примитивного элемента $\alpha = a$ в степени с учетом того, что операции выполняются по двойному модулю ($f(a)$, 3).

Решение к задаче 2.15.

1) Проведем последовательное возведение в степень элемента $\alpha = a$ с учетом того, что операции выполняются по двойному модулю ($f(a)$, 2):

$\alpha^0 = 1$;

$\alpha^1 = a$;

$\alpha^2 = a^2$;

$\alpha^3 = a^2 + 1$;

$\alpha^4 = a^2 + a + 1$;

$\alpha^5 = a + 1$;

$\alpha^6 = a^2 + a$.

Для обозначения нулевого элемента поля используется формальная запись $\alpha^{-\infty} = 0$.

2) Очевидно, что период элемента a равен $\varepsilon(a)=7$, т.е. равен $\varepsilon_{max}=2^3-1$ – порядку мультипликативной группы поля. Свойство цикличности группы проявляется в том, что $\alpha^7 = \alpha^0 = 1$, $\alpha^8 = \alpha^1$, $\alpha^9 = \alpha^2$ и т.д.

Целочисленная	Степенная	Полиномиальная	Векторная
0	$\alpha^{-\infty}$	0	0 0 0
1	α^0	1	0 0 1
2	α^1	a	0 1 0
3	α^2	a^2	1 0 0
4	α^3	$a^2 + 1$	0 1 1
5	α^4	$a^2 + a + 1$	1 1 0
6	α^5	$a + 1$	1 1 1
7	α^6	$a^2 + a$	1 0 1

Решение к задаче 2.16.

1) Переходим к степенной форме и раскрываем скобки

$(\alpha^6x^4+\alpha^3x^3+x+\alpha)(\alpha^2x+\alpha^3)=\alpha^8x^5+\alpha^5x^4+\alpha^2x^2+\alpha^3x+\alpha^9x^4+\alpha^6x^3+\alpha^3x+$

$+\alpha^4 = \alpha x^5+(\alpha^5+\alpha^2)x^4+\alpha^6x^3+\alpha^2x^2+(\alpha^3+\alpha^3)x+\alpha^4.$

2) Слагаемые в скобках представляем в полиномиальной форме, выполняем сложение по mod 2 и переходим обратно к степенной форме

$$\alpha^5+\alpha^2 = a^2+a+1+a^2 = a+1 = \alpha^3;\ \alpha^3+\alpha^3 = 0;$$

$$A(x) = \alpha x^5+\alpha^3x^4+\alpha^6x^3+\alpha^2x^2+\alpha^4.$$

3) Вычисляем остаток от деления $A(x)$ на $f(x)$

$$\begin{array}{l} \alpha x^5+\alpha^3x^4+\alpha^6x^3+\alpha^2x^2+\alpha^4 \,\big|\, x^3+x+1 \\ \ominus\ \underline{\alpha x^5+\alpha x^3+\alpha x^2\qquad\qquad\quad} \\ \alpha^3x^4+\alpha^5x^3+\alpha^4x^2+\alpha^4 \\ \ominus\ \underline{\alpha^3x^4+\alpha^3x^2+\alpha^3x\qquad} \\ \alpha^5x^3+\alpha^6x^2+\alpha^3x+\alpha^4 \\ \underline{\alpha^5x^3+\alpha^5x+\alpha^5} \\ \alpha^6x^2+\alpha^2x+1 = R(x),\ R(x) = A(x) \bmod f(x). \end{array}$$

4) Находим значение полинома $R(x)$, и соответственно $A(x)$, в точке $x = 5 = \alpha^4$.

$R(\alpha^4) = \alpha^6(\alpha^4)^2+\alpha^2\alpha^4+1 = \alpha^{14}+\alpha^6+1 = 1+\alpha^6+1 = \alpha^6 = 7$.

Ответ: $A(5) = 7$.

Решение к задаче 2.17.

1) Переходим к степенной форме и раскрываем скобки

$(\alpha^6x^4+\alpha^3x^3+x+\alpha)(\alpha^2x+\alpha^3)=\alpha^8x^5+\alpha^5x^4+\alpha^2x^2+\alpha^3x+\alpha^9x^4+\alpha^6x^3+\alpha^3x+$

$+\alpha^4 = \alpha x^5+(\alpha^5+\alpha^2)x^4+\alpha^6x^3+\alpha^2x^2+(\alpha^3+\alpha^3)x+\alpha^4.$

2) Слагаемые в скобках представляем в полиномиальной форме, выполняем сложение по mod 2 и переходим обратно к степенной форме

$$\alpha^5+\alpha^2 = a^2+a+1+a^2 = a+1 = \alpha^3;\ \alpha^3+\alpha^3 = 0;$$

$$A(x) = \alpha x^5+\alpha^3x^4+\alpha^6x^3+\alpha^2x^2+\alpha^4.$$

3) Вычисляем $A(x)$ modd $(f(x),2)$, т.е. находим остаток от деления $A(x)$ на $f(x)$

$$\begin{array}{l} \alpha x^5+\alpha^3x^4+\alpha^6x^3+\alpha^2x^2+\alpha^4 \,\big|\, x^3+x+1 \\ \ominus\ \underline{\alpha x^5+\alpha x^3+\alpha x^2\qquad\qquad\quad} \\ \alpha^3x^4+\alpha^5x^3+\alpha^4x^2+\alpha^4 \\ \ominus\ \underline{\alpha^3x^4+\alpha^3x^2+\alpha^3x\qquad} \\ \alpha^5x^3+\alpha^6x^2+\alpha^3x+\alpha^4 \\ \underline{\alpha^5x^3+\alpha^5x+\alpha^5} \\ \alpha^6x^2+\alpha^2x+1 = R(x),\ R(x) = A(x) \bmod f(x). \end{array}$$

4) Находим значение полинома $R(x)$, и соответственно $A(x)$, в точке $x = 5 = \alpha^4$.

$R(\alpha^4) = \alpha^6(\alpha^4)^2+\alpha^2\alpha^4+1 = \alpha^{14}+\alpha^6+1 = 1+\alpha^6+1 = \alpha^6 = 7$.

Ответ: $A(5) = 7$.

Решение к задаче 2.18.

1) Переходим к степенной форме и раскрываем скобки

$(\alpha^6x^4+\alpha^3x^3+x+\alpha)(\alpha^2x+\alpha^3)=\alpha^8x^5+\alpha^5x^4+\alpha^2x^2+\alpha^3x+\alpha^9x^4+\alpha^6x^3+\alpha^3x+$
$+\alpha^4 = \alpha x^5+(\alpha^5+\alpha^2)x^4+\alpha^6x^3+\alpha^2x^2+(\alpha^3+\alpha^3)x+\alpha^4.$

2) Слагаемые в скобках представляем в полиномиальной форме, выполняем сложение по mod 2 и переходим обратно к степенной форме

$\alpha^5+\alpha^2 = a^2+a+1+a^2 = a+1 = \alpha^3$; $\alpha^3+\alpha^3 = 0$;

$A(x) = \alpha x^5+\alpha^3x^4+\alpha^6x^3+\alpha^2x^2+\alpha^4.$

3) Вычисляем $A(x)$ mod $f(x)$, т.е. находим остаток от деления $A(x)$ на $f(x)$

$$\begin{array}{ll} & \alpha x^5+\alpha^3x^4+\alpha^6x^3+\alpha^2x^2+\alpha^4 \,\big|\, x^3+x+1 \\ \ominus & \underline{\alpha x^5+\alpha x^3+\alpha x^2} \qquad\qquad\quad \big|\, \alpha x^2+\alpha^3x+\alpha^5 \\ \ominus & \alpha^3x^4+\alpha^5x^3+\alpha^4x^2+\alpha^4 \\ & \underline{\alpha^3x^4+\alpha^3x^2+\alpha^3x} \\ & \alpha^5x^3+\alpha^6x^2+\alpha^3x+\alpha^4 \\ & \underline{\alpha^5x^3+\alpha^5x+\alpha^5} \\ & \alpha^6x^2+\alpha^2x+1 = R(x),\ R(x) = A(x) \bmod f(x). \end{array}$$

4) Находим значение полинома $R(x)$, и соответственно $A(x)$, в точке $x = 5 = \alpha^4$

$R(\alpha^4) = \alpha^6(\alpha^4)^2+\alpha^2\alpha^4+1 = \alpha^{14}+\alpha^6+1 = 1+\alpha^6+1 = \alpha^6 = 7$.

5) Ответ: $A(5) = 7$.

Решение к задаче 2.19.

а) $\varepsilon(\alpha^{25}) = \dfrac{63}{\text{НОД}(25,63)} = 63;$

б) $\varepsilon(\alpha^{14}) = \dfrac{63}{\text{НОД}(14,63)} = 9;$

в) $\varepsilon(\alpha^{36}) = \dfrac{63}{\text{НОД}(36,63)} = 7;$

г) $\varepsilon(\alpha^{19}) = \dfrac{63}{\text{НОД}(19,63)} = 63;$

д) $\varepsilon(\alpha^{45}) = \dfrac{63}{\text{НОД}(45,63)} = 7;$

е) $\varepsilon(\alpha^{12}) = \dfrac{63}{\text{НОД}(12,63)} = 21.$

Решение к задаче 2.20.

1)

Степенная	Полиномиальная	Степенная	Полиномиальная
$\alpha^{-\infty}$	0	α^7	a^3+a+1
α^0	1	α^8	a^2+1
α^1	a	α^9	a^3+a
α^2	a^2	α^{10}	a^2+a+1

Степенная	Полиномиальная	Степенная	Полиномиальная
α^3	a^3	α^{11}	a^3+a^2+a
α^4	$a+1$	α^{12}	a^3+a^2+a+1
α^5	a^2+a	α^{13}	a^3+a^2+1
α^6	a^3+a^2	α^{14}	a^3+1

2) Определить число k различных p-сопряженных элементов для элементов α^4: $\alpha^4\,\alpha^8\alpha^1\alpha^2$; α^6: $\alpha^6\,\alpha^{12}\alpha^9\alpha^3$.

3) Определить минимальные полиномы для элементов

$\alpha^2\,\alpha^4\,\alpha^8\alpha^1$

$$m_{\alpha^2}(x)=m_{\alpha^4}(x)=m_{\alpha^8}(x)=m_{\alpha^1}(x)=(x-\alpha^2)(x-\alpha^4)(x-\alpha^8)(x-\alpha^1)=$$

$$=(x^2-x(\alpha^2+\alpha^8)+\alpha^2\alpha^8)\times(x^2-x(\alpha^1+\alpha^4)+\alpha^1\alpha^4)=$$

$$=(x^2+x+\alpha^{10})(x^2+x+\alpha^5)=x^4+\underline{x^3}+\alpha^5x^2+\underline{x^3}+x^2+\alpha^5x+$$

$$+\alpha^{10}x^2+\alpha^{10}x+\alpha^0=x^4+x^2(\alpha^5+1+\alpha^{10})+x(\alpha^5+\alpha^{10})+1=x^4+x+1$$

$\alpha^5\,\alpha^{10}$

$$m_{\alpha^5}(x)=m_{\alpha^{10}}(x)=(x-\alpha^5)(x-\alpha^{10})=x^2-x(\alpha^5+\alpha^{10})+\alpha^5\alpha^{10}=x^2+x+1.$$

Решение к задаче 2.21.

1)

Степенное	Полиномиальное	Степенное	Полиномиальное
$\alpha^{-\infty}$	0	α^7	a^3+a+1
α^0	1	α^8	a^2+1
α^1	a	α^9	a^3+a
α^2	a^2	α^{10}	a^2+a+1
α^3	a^3	α^{11}	a^3+a^2+a
α^4	$a+1$	α^{12}	a^3+a^2+a+1
α^5	a^2+a	α^{13}	a^3+a^2+1
α^6	a^3+a^2	α^{14}	a^3+1

2) Определить число k различных p-сопряженных элементов для элементов α^4: $\alpha^4\,\alpha^8\alpha^1\alpha^2$; α^6: $\alpha^6\,\alpha^{12}\alpha^9\alpha^3$.

3) Определить минимальные полиномы для элементов

$\alpha^2\,\alpha^4\,\alpha^8\alpha^1$

$$m_{\alpha^2}(x)=m_{\alpha^4}(x)=m_{\alpha^8}(x)=m_{\alpha^1}(x)=(x-\alpha^2)(x-\alpha^4)(x-\alpha^8)(x-\alpha^1)=$$

$$=(x^2-x(\alpha^2+\alpha^8)+\alpha^2\alpha^8)\times(x^2-x(\alpha^1+\alpha^4)+\alpha^1\alpha^4)=$$

$$=(x^2+x+\alpha^{10})(x^2+x+\alpha^5)=x^4+\underline{x^3}+\alpha^5x^2+\underline{x^3}+x^2+\alpha^5x+\alpha^{10}x^2+\alpha^{10}x+\alpha^0=$$

$$=x^4+x^2(\alpha^5+1+\alpha^{10})+x(\alpha^5+\alpha^{10})+1=x^4+x+1$$

$\alpha^5\,\alpha^{10}$

$$m_{\alpha^5}(x)=m_{\alpha^{10}}(x)=(x-\alpha^5)(x-\alpha^{10})=x^2-x(\alpha^5+\alpha^{10})+\alpha^5\alpha^{10}=x^2+x+1$$

Решение к задаче 2.22.

а) $\pi(x)= x^2+x+2$; $i=3$; $j=5$;

б) $\pi(x)= x^2+2x+2$; $i=3$; $j=5$;

в) $\pi(x)= x^2+x+2$; $i=5$; $j=7$;

г) $\pi(x)= x^2+2x+2$; $i=5$; $j=7$;

д) $\pi(x)= x^2+x+2$; $i=7$; $j=3$;

е) $\pi(x)= x^2+2x+2$; $i=7$; $j=3$.

Построить расширенное поле $GF(3^2)$, определить функцию следа, минимальный полином, аддитивный и мультипликативный характеры для заданного элемента поля.

а), в), д)

1) Построение поля.

$GF(3^2)$, $\pi(x) = x^2+x+2$, $\alpha = a$			Автоморфные поля			
ЦП	α^i	**ПП**	β^j	$\beta = \alpha^3$	$\beta = \alpha^5$	$\beta = \alpha^7$
0	$\alpha^{-\infty}$	0	$\beta^{-\infty}$	0	0	0
1	α^0	1	β^0	1	1	1
2	α^1	a	β^1	$2a+2$	$2a$	$a+1$
3	α^2	$2a+1$	β^2	$a+2$	$2a+1$	$a+2$
4	α^3	$2a+2$	β^3	a	$a+1$	$2a$
5	α^4	2	β^4	2	2	2
6	α^5	$2a$	β^5	$a+1$	a	$2a+2$
7	α^6	$a+2$	β^6	$2a+1$	$a+2$	$2a+1$
8	α^7	$a+1$	β^7	$2a$	$2a+2$	a

2) Функция следа, минимальный полином, аддитивный и четырехзначный мультипликативный характеры ($M = 4$, $\mu = 1$) для элемента β^5 (вариант а).

Функция следа

$$\mathrm{tr}_{n1}a = \sum_{i=0}^{n-1} a^{p^i};$$

$$\mathrm{tr}_{21}\beta^5 = \sum_{i=0}^{n-1=1} (\beta^5)^{p^i} = \beta^5 + \beta^{15 \bmod 8} = \beta^5 + \beta^7 = a + 1 + 2a = 1;$$

минимальный полином

$$m_a(x) = \prod_{i=0}^{k-1} \left(x - a^{p^i} \right);$$

$$m(x) = (x-\beta^5)(x-\beta^7) = x^2-(\beta^5+\beta^7)x+\beta^{12} = x^2+2x+2;$$

аддитивный характер

$$e(a) = \exp(j2\pi \mathrm{tr}_{n1}\mu a/p);$$

$$e(\beta^5) = \exp(j2\pi \mathrm{tr}_{21}\beta^5/3) = \exp(j2\pi/3);$$

мультипликативный M-значный характер

$$\psi(a) = \exp(j2\pi \log_\alpha a/M);$$

$$\psi(\beta^5) = \exp(j2\pi \log_\beta \beta^5/M) = \exp(j5\pi/2) = \exp(j\pi/2) = +j.$$

Результаты вычислений для вариантов в) и д) сведены в таблицу.

Вариант	j	$\mathrm{tr}_{21}\beta^j$	$m(x)$	$e(\beta^j)$	$\psi(\beta^j)$
а)	5	1	x^2+2x+2	$\exp(j2\pi/3)$	$+j$
в)	7	2	x^2+x+2	$\exp(j4\pi/3)$	$-j$
д)	3	1	x^2+2x+2	$\exp(j2\pi/3)$	$-j$

б), г), е)

1) Построение поля.

$GF(3^2)$, $\pi(x)=x^2+x+2$, $\alpha=a$			Автоморфные поля			
ЦП	α^i	ПП	β^j	$\beta=\alpha^3$	$\beta=\alpha^5$	$\beta=\alpha^7$
0	$\alpha^{-\infty}$	0	$\beta^{-\infty}$	0	0	0
1	α^0	1	β^0	1	1	1
2	α^1	a	β^1	$2a+1$	$2a$	$a+2$
3	α^2	$a+1$	β^2	$2a+2$	$a+1$	$2a+2$
4	α^3	$2a+1$	β^3	a	$a+2$	$2a$
5	α^4	2	β^4	2	2	2
6	α^5	$2a$	β^5	$a+2$	a	$2a+1$
7	α^6	$2a+2$	β^6	$a+1$	$2a+2$	$a+1$
8	α^7	$a+2$	β^7	$2a$	$2a+1$	a

2) Функция следа, минимальный полином, аддитивный и четырехзначный мультипликативный характеры ($M=4$, $\mu=1$).

Номер варианта	j	$\mathrm{tr}_{21}\beta^j$	$m(x)$	$e(\beta^j)$	$\psi(\beta^j)$
б)	5	2	x^2+x+2	$\exp(j4\pi/3)$	$+j$
г)	7	1	x^2+2x+2	$\exp(j2\pi/3)$	$-j$
е)	3	2	x^2+x+2	$\exp(j4\pi/3)$	$-j$

Решение к задаче 2.23.

1. Значение полинома $A(x)$ в точке $x=5$ можно было находить непосредственно после пункта 2 без выполнения операции сравнения по модулю $f(x)$; результат должен быть тот же самый. Покажем это:

$$A(\alpha^4)=\alpha(\alpha^4)^5+\alpha^3(\alpha^4)^4+\alpha^6(\alpha^4)^3+\alpha^2(\alpha^4)^2+\alpha^4=\alpha^{21}+\alpha^{19}+\alpha^{18}+\alpha^{10}+\alpha^4=$$
$$=1+a^2+a+1+a+1=a^2+1=\alpha^6=7.$$

2. При выполнении операции деления полинома на полином и сложении (вычитании) коэффициентов при одинаковых степенях x также осуществляется переход к полиномиальной форме.

3. Упрощенное выражение имеет вид

$$A(x)=R(x)=7x^2+3x+1$$

Решение к задаче 2.24.

1) $p^n-1=15$, $\varepsilon(\alpha^3)=\dfrac{15}{\text{НОД}(3,15)}=5$; 2) $\varepsilon(\alpha^5)=\dfrac{15}{\text{НОД}(5,15)}=3$;

3) $\varepsilon(\alpha^7)=\dfrac{15}{\text{НОД}(7,15)}=15$; 4) $\varepsilon(\alpha^{14})=\dfrac{15}{\text{НОД}(14,15)}=15$;

5) элементы α^7 и α^{14} являются примитивными.

Решение к задаче 2.25.

1) $\varepsilon(\alpha^4) = \dfrac{63}{\text{НОД}(4,63)} = 63$; 2) $\varepsilon(\alpha^{27}) = \dfrac{63}{\text{НОД}(27,63)} = 7$;

3) $\varepsilon(\alpha^{42}) = \dfrac{63}{\text{НОД}(42,63)} = 3$; 4) $\varepsilon(\alpha^{49}) = \dfrac{63}{\text{НОД}(49,63)} = 9$;

5) $\varepsilon(\alpha^{57}) = \dfrac{63}{\text{НОД}(57,63)} = 21$; 6) $\varepsilon(\alpha^0 = \alpha^{63}) = \dfrac{63}{\text{НОД}(63,63)} = 1$.

Решение к задаче 2.26.

1) $N_1 = 1$;

2) N_3: $3 = 1\cdot 3$; $N_3 = 3^0\cdot(3-1) = 2$;

3) N_7: $7 = 1\cdot 7$; $N_7 = 7^0\cdot(7-1) = 6$;

4) N_9: $9 = 1\cdot 3^2$; $N_9 = 3^1\cdot(3-1) = 6$;

5) N_{21}: $21 = 1\cdot 3\cdot 7$; $N_{21} = 3^0\cdot(3-1)\cdot 7^0\cdot(7-1) = 12$;

6) N_{63}: $63 = 1\cdot 3^2\cdot 7$; $N_{63} = 3^1\cdot(3-1)\cdot 7^0\cdot(7-1) = 36$.

Решение к задаче 2.27.

1) $\varepsilon(\alpha^{-1}) = \varepsilon(\alpha^{14}) = \dfrac{2^4-1}{\text{НОД}(14,15)} = 15$;

2) $\varepsilon(\alpha^{-4}) = \varepsilon(\alpha^{11}) = \dfrac{15}{\text{НОД}(11,15)} = 15$;

3) $\varepsilon(\alpha^{-7}) = \varepsilon(\alpha^{8}) = \dfrac{15}{\text{НОД}(8,15)} = 15$;

4) $\varepsilon(\alpha^{-13}) = \varepsilon(\alpha^{2}) = \dfrac{15}{\text{НОД}(2,15)} = 15$.

Решение к задаче 2.28.

1) Построение поля с примитивным элементом $\alpha = a$:

$\alpha^{-\infty} = 0$,

$\alpha^0 = 1$,

$\alpha^1 = a$,

$\alpha^2 = a+1$.

2) Проверка выполнения теоремы Ферма. Пусть $x = \alpha^2$, тогда $(\alpha^2)^4 - \alpha^2 = \alpha^{8 \bmod 3} - \alpha^2 = 0$.

3) $\prod_{i=1}^{p^n}(x - a_i) = (x-0)(x-1)(x-a)(x-a-1) \bmod (a^2+a+1) =$

$= (x^2-x)(x^2+a^2+x+a) \bmod (a^2+a+1) = x(x+1)(x^2+x+1) = x^4+x$.

Решение к задаче 2.29.

1. Порядок мультипликативной группы $L = 2^4-1 = 15 = = 1\cdot 3\cdot 5$; следовательно существует один элемент с периодом $\varepsilon = 1$, два элемента с периодом $\varepsilon = 3$, четыре элемента с периодом $\varepsilon = 5$ и восемь элементов с периодом $\varepsilon_{max} = 15$.

2. Подгруппа H_1 порядка $L = 1$ – это есть тривиальная подгруппа $H_1 = \{1\}$.

3. Подгруппа H_2 порядка $L = 3$ – состоит из двух элементов с периодом $\varepsilon = 3$ и нейтрального элемента по умножению $e = 1$, т.е. $H_2 = \{1, \alpha^5, \alpha^{10}\}$.

4. Подгруппа H_3 порядка $L = 5$ – состоит из элементов с периодом $\varepsilon = 5$ и нейтрального элемента по умножению $H_3 = \{1, \alpha^3, \alpha^6, \alpha^9, \alpha^{12}\}$.

5. Оставшиеся восемь элементов (α, α^2, α^4, α^8, α^7, α^{11}, α^{13}, α^{14}) являются примитивными и входят только в основную группу $G_\times$.

Решение к задаче 2.30.

1. В качестве образующего элемента a_i смежного класса можно выбрать произвольный элемент группы G. Возможны два варианта:

а) $a_i \in H$: в этом случае смежные классы совпадают с подгруппой H, например, если $a_1 = \alpha^9$, то $a_1H = \{\alpha^9, \alpha^3\cdot\alpha^9, \alpha^6\cdot\alpha^9, \alpha^9\cdot\alpha^9, \alpha^{12}\cdot\alpha^9\} = \{\alpha^9, \alpha^{12}, 1, \alpha^3, \alpha^6\} = H$;

б) $a_i \notin H$: в этом случае смежные классы не совпадают с подгруппой H, например, если $a_2 = \alpha^2 \notin H$, то $a_2H = \{\alpha^2, \alpha^2\cdot\alpha^3, \alpha^2\cdot\alpha^6, \alpha^2\cdot\alpha^9, \alpha^{12}\cdot\alpha^9\} = \{\alpha^2, \alpha^5, \alpha^8, \alpha^{11}, \alpha^{14}\}$.

2. Так как группа G имеет порядок $L = 15$, то она может быть представлена как объединение трех непересекающихся смежных классов. В качестве первого выступает a_1H, совпадающий с подгруппой H, в качестве второго – a_2H.

Образующим элементом третьего смежного класса целесообразно выбирать элемент, не входящий в первые два класса. Например, если $a_3 = \alpha$, то $a_3H = \{\alpha, \alpha^4, \alpha^7, \alpha^{10}, \alpha^{13}\}$. В результате имеем

$$G = \{a_1H\} + \{a_2H\} + \{a_3H\},$$

где символ сложения следует рассматривать как символ объединения.

Решение к задаче 2.31.

1. Разложим степень расширения $n = 18$ простого поля $GF(2)$ на множители $n = 18 = 2\cdot2\cdot3$.

2. Определим различные подполя: $GF(2)$, $GF(2^2)$, $GF(2^3)$, $GF(2^6)$, $GF(2^9)$.

Таким образом, поле $GF(2^{18})$ содержит 5 подполей.

Решение к задаче 2.32.

1. Разложим степень расширения $n = 18$ простого поля $GF(2)$ на множители: $n = 18 = 2\cdot3\cdot3$.

2. Определим различные подполя:

$GF(2)$, $GF(2^2)$, $GF(2^3)$, $GF(2^6)$, $GF(2^9)$.

Таким образом, поле $GF(2^{18})$ содержит 5 подполей.

Решение к задаче 2.33.

1. $GF(2^3)$: $(\alpha^j)^{2^i}$, $i = 0,1,2,\ldots$.

α^j	$i=0$	$i=1$	$i=2$	$i=3$	k
α	α^1	α^2	α^4	$\alpha^8=\alpha^1$	3
α^3	α^3	α^6	$\alpha^{12}=\alpha^5$	$\alpha^{10}=\alpha^3$	3
α^4	α^4	$\alpha^8=\alpha^1$	α^2	α^4	3
α^5	α^5	$\alpha^{10}=\alpha^3$	α^6	$\alpha^{12}=\alpha^5$	3
α^6	α^6	$\alpha^{12}=\alpha^5$	$\alpha^{10}=\alpha^3$	α^6	3
α^0	α^0	α^0			1

2. $GF(3^2)$: $(\alpha^j)^{3^i}$, $i = 0,1,2,\ldots$

α^j	$i=0$	$i=1$	$i=2$	k
α^1	α^1	α^3	$\alpha^9=\alpha^1$	2
α^3	α^3	$\alpha^9=\alpha^1$	α^3	2
α^4	α^4	$\alpha^{12}=\alpha^4$		1
α^5	α^5	$\alpha^{15}=\alpha^7$	$\alpha^{21}=\alpha^5$	2
α^6	α^6	$\alpha^{18}=\alpha^2$	α^6	2
α^0	α^0	α^0		1

3. $GF(2^4)$: $(\alpha^j)^{2^i}$, $i = 0,1,2,...$

α^j	$i = 0$	$i = 1$	$i = 2$	$i = 3$	$i = 4$	k
α	α^1	α^2	α^4	α^8	$\alpha^{16}=\alpha^1$	4
α^3	α^3	α^6	α^{12}	$\alpha^{24}=\alpha^9$	$\alpha^{18}=\alpha^3$	4
α^4	α^4	α^8	$\alpha^{16}=\alpha^1$	α^2	α^4	4
α^5	α^5	α^{10}	$\alpha^{20}=\alpha^5$			2
α^6	α^6	α^{12}	$\alpha^{24}=\alpha^9$	$\alpha^{18}=\alpha^3$	α^6	4
α^0	α^0	α^0				1

Решение к задаче 2.34.

1. Построение поля $GF(2^3)$:

$\alpha^{-\infty} = 0$, $\alpha^0 = 1$, $\alpha^1 = a$, $\alpha^2 = a^2$, $\alpha^3 = a+1$, $\alpha^4 = a^2+a$, $\alpha^5 = a^2+a+1$, $\alpha^6 = a^2+1$.

2. *Определение p*-сопряженных элементов:

а) α, α^2, α^4; $k = 3$;

б) α^3, α^6, α^5; $k = 3$;

в) $\alpha^{-\infty} = 0$; $k = 1$;

г) $\alpha^0 = 1$; $k = 1$.

3. Вычисление минимальных полиномов:

а) $m_\alpha(x) = m_{\alpha^2}(x) = m_{\alpha^4}(x) = (x-\alpha)(x-\alpha^2)(x-\alpha^4) =$

$= \left(x^2 - (\alpha+\alpha^2)x + \alpha^3\right)(x-\alpha^4) = (x^2 - \alpha^4 x + \alpha^3)(x-\alpha^4) =$

$= x^3 - (\alpha^4+\alpha^4)x^2 + (\alpha^3+\alpha)x - \alpha^7 = x^3 + x + 1,$

так как в полях характеристики $p = 2$ знаки «–» и «+» эквиваленты;

б) $m_{\alpha^3}(x) = m_{\alpha^5}(x) = m_{\alpha^6}(x) = (x-\alpha^3)(x-\alpha^5)(x-\alpha^6) = x^3+x^2+1$;

в) $m_0(x) = (x-0) = x$;

г) $m_{\alpha^0}(x) = (x-1) = x+1$.

Решение к задаче 2.35.

1. Построение поля $GF(3^2)$.

$\alpha^0 = 1$,

$\alpha^1 = a$,

$\alpha^2 = a^2$ modd($f(a)$,3) = $2a+1$,

$\alpha^3 = (2a+1)a$ modd($f(a)$,3) = $2a+2$,

$\alpha^4 = (2a+2)a$ modd($f(a)$,3) = 2,

$\alpha^5 = 2a$,

$\alpha^6 = 2a^2$ modd($f(a)$,3) = $a+2$,

$\alpha^7 = (a+2)a = a+1$.

2. Разбиение на группы *p*-сопряженных элементов

а) α^0; б) α^1,α^3; в) α^2,α^6; г) α^4; д) α^5,α^7.

3. Вычисление минимальных полиномов

а) $m_0(x) = x$, $m_1(x) = x-1 = x+2$;

б) $m_{\alpha^1}(x) = m_{\alpha^3}(x) = (x-\alpha^1)(x-\alpha^3) = x^2-(\alpha^1-\alpha^3)x+\alpha^4 =$

$= x^2-2x+2 = x^2+x+2$;

в) $m_{\alpha^2}(x) = m_{\alpha^6}(x) = (x-\alpha^2)(x-\alpha^6) = x^2 - 0x + 1 = x^2 + 1$;

г) $m_{\alpha^4}(x) = x - \alpha^4 = x - 2 = x + 1$;

д) $m_{\alpha^5}(x) = m_{\alpha^7}(x) = x^2 - 2x + 2$.

Очевидно, что $x^9 - x = x(x+2)(x^2+x+2)(x^2+1)\ (x+1)(x^2+2x+2)$.

Все минимальные полиномы являются неприводимыми над полем $GF(3)$. Минимальные полиномы $m_{\alpha^1}(x)$ и $m_{\alpha^5}(x)$ еще и примитивные, так как период их корней равен $\varepsilon_{max} = 3^2 - 1 = 8$ – порядку мультипликативной группы поля $GF(3^2)$. Неприводимый полином $m_{\alpha^2}(x)$ степени $k = 2$ не является примитивным, так как период его корней равен $\varepsilon(\alpha^2) = 4$.

Решение к задаче 2.36.

1. $GF(2^4)$, $f(x) = x^4+x+1$, $\alpha = a$:

$f_1^*(x) = x^4 \cdot 1^{-1}(x^{-4} + x^{-1} + 1) = 1 + x^3 + x^4$;

$f_2^*(x) = x^4 \cdot 1^{-1}(x^{-4} + x^{-3} + x^{-2} + x^{-1} + 1) = 1 + x + x^2 x^3 + x^4 = f_2(x)$.

Корнями полинома $f_1(x)$ являются элементы α^1, α^2, α^4, α^8, тогда корнями $f_1^*(x)$ будут $\alpha^{-1} = \alpha^{14}$, $\alpha^{-2} = \alpha^{13}$, $\alpha^{-4} = \alpha^{11}$, $\alpha^{-8} = \alpha^7$. Полиномы $f_2(x)$ и $f_2^*(x)$ совпадают, их корни α^3, α^6, α^9, α^{12}, и $\alpha^{-3} = \alpha^{12}$, α^9, α^6, α^3 соответственно равны. Такие полиномы называются самосопряженными.

2. $GF(3^2)$, $f(x) = x^2+x+2$, $\alpha = a$:

$f_3^*(x) = x^2 \cdot 2^{-1}(x^{-2} + 2x^{-1} + 2) = 2 + x + x^2$, так как $2^{-1} = 2 \bmod 3$;

корни $f_3(x)$ (см. решение к задаче 2.20 п.3): α^5, α^7; корни $f_3^*(x)$: $\alpha^1 = \alpha^{-7}$ и $\alpha^3 = \alpha^{-5}$;

$f_4^*(x) = x^2 \cdot 1^{-1}(x^{-2} + 1) = 1 + x^2 = f_4(x)$, корни α^2, α^6;

$f_5^*(x) = x \cdot 2^{-1}(x^{-1} + 2) = 2 + x = f_5(x)$, корень $\alpha^0 = 1$.

Решение к задаче 2.37.

Умножение в поле $GF(2^2)$ $f_n(a) = a^2+a+1$

⊗	0	1	a	a+1
0	0	0	0	0
1	0	1	a	a+1
a	0	a	a+1	1
a+1	0	a+1	1	a

1. При вычислении элементов поля $GF[(2^2)^2]$ потребуется таблица умножения элементов поля $GF(2^2)$. Так как в качестве примитивного элемента поля с двойным расширением взят элемент $\alpha = x$, то полином $f_s(z)$, неприводимый над $GF(2^2)$, записывается относительно формальной переменной z.

Построение поля целесообразно проводить возведением в последовательные степени примитивного элемента $\alpha = x$.

$\alpha^0 = 1$; $\alpha^1 = x$; $\alpha^2 = x^2 \bmod(x^2+x+a,\ a^2+a+1,2) = x+a$;

$\alpha^3 = (x+a)x = x^2+ax \bmod(f_s(x),\ f_n(a),2) = x+a+ax = (a+1)x+a$;

$\alpha^4 = (a+1)x^2+ax = (a+1)(x+a)+ax = \underline{ax}+x+a+a^2+\underline{ax} \bmod(f_s(x),f_n(x),2) =$

$= x+a+a+1 = x+1$; ... .

Вычисление произвольного элемента поля, например $\alpha^9 = = x^9$, реализуется путем нахождения остатка от деления x^9 на полином $f_s(x) = x^2+x+a$. При этом промежуточные операции при делении «столбиком» выполняются с учетом полинома $f_n(a) = a^2+a+1$, т.е. $a^2 = a+1 \bmod (a^2+a+1)$

$$\alpha^9 = x^9 \operatorname{modd}(f_s(x), f_n(a), 2) = R(x) = ax + a,$$

так как

$$\begin{array}{l}
\oplus\ x^9 \quad \left|\begin{array}{l} x^2+x+a \\ \hline x^7+x^6+(a+1)x^5+x^4+ax^2+ax+1 \end{array}\right. \\
\underline{x^9+x^8+ax^7} \\
\oplus\ x^8+ax^7 \\
\underline{x^8+x^7+ax^6} \\
\oplus\ (a+1)x^7+ax^6 \\
\underline{(a+1)x^7+(a+1)x^6+a(a+1)x^5} \\
\oplus\ x^6+x^5 \\
\underline{x^6+x^5+ax^4} \\
\oplus\ ax^4 \\
\underline{ax^4+ax^3+a^2x^2} \\
\oplus\ ax^3+(a+1)x^2 \\
\underline{ax^3+ax^2+a^2x} \\
\oplus\ x^2+(a+1)x \\
\underline{x^2+x+a} \\
ax+a = R(x).
\end{array}$$

Аналогично вычисляются остальные элементы поля $GF[(2^2)^2]$ вплоть до элемента $\alpha^{14} = (a+1)x+a+1$. Результаты сведены в первые пять граф табл. 2.1. В отличие от полей $GF(p^n)$ векторная форма элементов в полях с двойным расширением $GF[(p^n)^s]$ может быть представлена двумя способами. Во-первых, векторами размерности $s = 2$, координаты которых являются элементами поля $GF(2^2)$, $f_n(a) = a^2+a+1$. Во-вторых, векторами размерности $ns = 4$, координаты которых принимают значения из простого поля $GF(2)$.

2. Особенность вычисления минимальных полиномов в полях с двойным расширением заключается в том, что их корнями являются не p-сопряженные, а q-сопряженные элементы поля $GF[(p^n)^s]$, где $q = p^n$. Соответственно коэффициентами минимальных полиномов являются элементы поля $GF(p^n)$. Определим минимальные полиномы для элементов α^2, α^5, α^9 и α^{11} поля $GF[(2^2)^2]$, степень которых равна числу k различных q–сопряженных элементов ($q = 2^2 = 4$), $(\alpha^i)^{q^j}$ ($j = 0,1,2,...$):

	$j = 0$	$j = 1$	$j = 2$	k
$(\alpha^2)^{4^j}$	α^2	α^8	$\alpha^{32} = \alpha^2$	2
$(\alpha^5)^{4^j}$	α^5	$\alpha^{20} = \alpha^5$		1
$(\alpha^9)^{4^j}$	α^9	$\alpha^{36} = \alpha^6$	$\alpha^{24} = \alpha^9$	2
$(\alpha^{11})^{4^j}$	α^{11}	$\alpha^{44} = \alpha^{14}$	$\alpha^{56} = \alpha^{11}$	2

$$m_{\alpha^2}(z) = (z-\alpha^2)(z-\alpha^8) = z^2 + (\alpha^2+\alpha^8)z + \alpha^{10} = z^2 + (x+a+x+a+1)z + a + 1 =$$

$$= z^2 + z + a + 1;$$

$$m_{\alpha^5}(z) = z - \alpha^5 = z + a;$$

$$m_{\alpha^9}(z) = (z-\alpha^9)(z-\alpha^6) = z^2 + (\alpha^9+\alpha^6)z + \alpha^{15} = z^2 + az + 1;$$

$$m_{\alpha^{11}}(z) = (z-\alpha^{11})(z-\alpha^{14}) = z^2 + (\alpha^{11}+\alpha^{14})z + \alpha^{25} = z^2 + (a+1)z + a + 1.$$

Таблица 2.1

Формы представления элементов поля $GF[(2^2)^2]$, $f_s(z) = z^2+z+a$, $f_n(a) = a^2+a+1$, $\alpha = x$					**Период элемента $\varepsilon(\alpha^i)$**	**Минимальные полиномы $m_a(z)$**	**Функция следа**	
Целочисл.	**Степенная**	**Полиномиальная**	**Векторная**					
			над $GF(2^2)$	**над $GF(2)$**			$tr_{41}\alpha$	$tr_{42}\alpha$
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
0	$\alpha^{-\infty}$	0	0 ,0	000	1	z	0	0
1	α^0	1	0, 1	0001	1	$z+1$	0	0
2	α^1	x	1, 0	0100	15	z^2+z+a	0	1
3	α^2	$x+a$	1, a	0110	15	$z^2+z+a+1$	0	1
4	α^3	$(a+1)x+a$	$a+1$, a	1110	5	$z^2+(a+1)z+1$	1	$a+1$
5	α^4	$x+1$	1, 1	0101	15	z^2+z+a	0	1
6	α^5	a	0, a	0010	3	$z+a$	0	0
7	α^6	ax	a, 0	1000	5	z^2+az+1	1	a
8	α^7	$ax+a+1$	a, $a+1$	1011	15	z^2+az+a	1	a
9	α^8	$x+a+1$	1, $a+1$	0111	15	$z^2+z+a+1$	0	1
10	α^9	$ax+a$	a, a	1010	5	z^2+az+1	1	a
11	α^{10}	$a+1$	0, $a+1$	0011	3	$z+a+1$	0	0
12	α^{11}	$(a+1)x$	$a+1$, 0	1100	15	$z^2+(a+1)z+a+1$	1	$a+1$
13	α^{12}	$(a+1)x+1$	$a+1$, 1	1101	5	$z^2+(a+1)z+1$	1	$a+1$
14	α^{13}	$ax+1$	a, 1	1001	15	z^2+az+a	1	a
15	α^{14}	$(a+1)x+a+1$	$a+1$, $a+1$	1111	15	$z^2+(a+1)z+a+1$	1	$a+1$

Показатели степеней элемента α сравниваются по модулю $(2^2)^2-1 = 15$. Результаты вычисления минимальных полиномов сведены в графу 7. Графы 8,9 будут пояснены ниже.

Решение к задаче 2.38.

а) $tr_{31}\alpha^0 = \alpha^0+(\alpha^0)^2+(\alpha^0)^4 = 1+1+1 = 1$;

б) $tr_{31}\alpha = \alpha+\alpha^2+\alpha^4 = a+a^2+a^2+a = 0$;

в) $tr_{31}\alpha^3 = (\alpha^3)^1+(\alpha^3)^2+(\alpha^3)^4 = \alpha^3+\alpha^6+\alpha^{12 \bmod 7} = 1$;

г) $tr_{31}\alpha^4 = \alpha^4+\alpha^8+\alpha^{16} = \alpha^4+\alpha+\alpha^2 = 0$.

Очевидно, что все p-сопряженные элементы имеют одинаковые следы. Поле $GF(2^3)$ имеет следующие циклотомические классы: {1,2,4}, {3,6,5}.

Решение к задаче 2.39.

1. Функции следа вычисляются для элементов поля $GF[(2^2)^2]$, представленных в таблице из решения задачи 2.37. Определим функции следа для элементов α^0, α^2, α^5, α^6, α^{13} в простом поле:

$$tr_{41}\alpha^0 = \sum_{i=0}^{3}(\alpha^0)^{2^i} = 1+1+1+1 = 0;$$

$$tr_{41}\alpha^2 = \alpha^2 + \alpha^4 + \alpha^8 + \alpha^1 = x + a + x + 1 + x + a + 1 + x = 0;$$

$$tr_{41}\alpha^5 = \alpha^5 + \alpha^{10} + \alpha^5 + \alpha^{10} = 0;$$

$$tr_{41}\alpha^6 = \alpha^6 + \alpha^{12} + \alpha^9 + \alpha^3 = ax + (a+1)x + 1 + ax + a + (a+1)x + a = 1;$$

$$tr_{41}\alpha^{13} = \alpha^{13} + \alpha^{11} + \alpha^7 + \alpha^{14} = ax + 1 + (a+1)x + ax + a + 1 + (a+1)x + a + 1 = 1.$$

Функции следа для тех же элементов в расширенном поле $GF(2^2)$:

$$tr_{42}\alpha^0 = \sum_{i=0}^{s-1}(\alpha^0)^{4^i} = 1+1 = 0;$$

$$tr_{42}\alpha^2 = \alpha^2 + \alpha^8 = x + a + x + a + 1 = 1;$$

$$tr_{42}\alpha^5 = \alpha^5 + \alpha^5 = 0;$$

$$tr_{42}\alpha^6 = \alpha^6 + \alpha^{24 \bmod 15} = \alpha^6 + \alpha^9 = ax + ax + a = a;$$

$$tr_{42}\alpha^{13} = \alpha^{13} + \alpha^{52 \bmod 15} = \alpha^{13} + \alpha^7 = ax + 1 + ax + a + 1 = a.$$

Результаты вычисления следов остальных элементов в простом и расширенном поле представлены в табл. 2.1 (графы 8, 9).

Наглядная интерпретация функции следа, рассмотренной в решении к задаче 2.24 в качестве отображения элементов расширенного поля в свое подполе представлена на рис. 2.1.

Элементы поля $GF[(2^2)^2]$ изображены точками на внешней окружности, а элементы подполей (простого $GF(2)$, рис. 2.1, *а*) и расширенного ($GF(2^2)$, рис. 2.1, *б*) – на внутренних окружностях. Функция следа изображается ребром, соединяющим точки внешней и внутренней окружностей. Например, значение следовой функции, равное a+1, имеют элементы α^3, α^{12}, α^{11}, α^{14}.

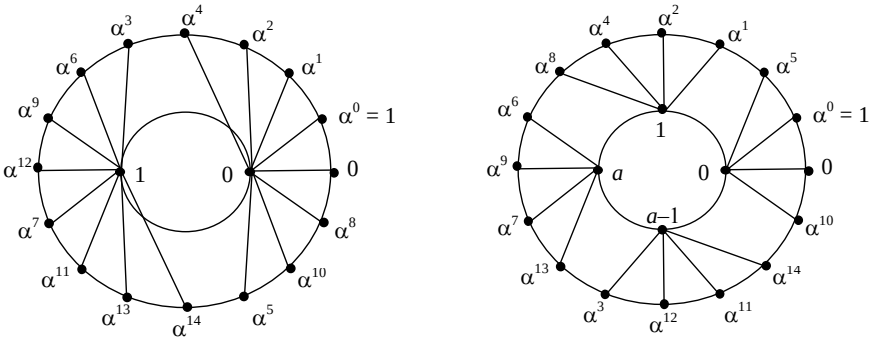

Рис. 2.1. Отображение элементов расширенного поля:
а) $GF[(2^2)^2] \Rightarrow GF(2)$; б) $GF[(2^2)^2] \Rightarrow GF(2^2)$

Функция следа используется при математическом описании процедуры синтеза кодовых псевдослучайных последовательностей, например, М-последовательностей, последовательностей Гордона-Миллса-Велча (ГМВ) [10,

21, 29]. Аналитическая запись для символов двоичной М–последовательности периода $N = 15$ имеет вид

$$a_i = tr_{41}\alpha^i,\ i = \overline{0, N-1},$$

где α – примитивный элемент поля $GF(2^4)$.

Для четверичной М-последовательности

$$b_i = tr_{42}\alpha^i,\ i = \overline{0, N-1}.$$

В таблице из решения к задаче 2.37 восьмая и девятая графы при считывании сверху вниз (за исключением строки, соответствующей нулевому элементу) соответствуют двоичной $МП_2$ и четверичной $МП_4$ М-последовательностям. При целочисленном представлении элементов поля ($a \sim 2$, $a+1 \sim 3$) они имеют вид

$МП_2$ = 000100110101111; $МП_4$ = 011310221203323.

Решение к задаче 2.40.

1. *Определение* следов элементов $tr_{21}\mu x$:

а) $tr_{21}\alpha^5\cdot\alpha = tr_{21}\alpha^6 = \alpha^6+\alpha^2 = 0$;

б) $tr_{21}\alpha^5\cdot\alpha^4 = tr_{21}\alpha^{9 \bmod 8} = tr_{21}\alpha = \alpha+\alpha^3 = 2$;

в) $tr_{21}\alpha^5\cdot\alpha^7 = tr_{21}\alpha^4 = \alpha^4+\alpha^4 = 2\alpha^4 = 2\cdot 2 = 1$.

2. Вычисление аддитивных характеров: а) $e(\alpha) = \exp(j2\pi\cdot 0/p) = 1$;

б) $e(\alpha^4) = \exp(j2\pi\cdot 2/3) = \exp(j\ 4\pi/3)$;

в) $e(\alpha^7) = \exp(j\ 2\pi/3)$.

Решение к задаче 2.41.

Порядок мультипликативной группы равен $L = p^n-1 = 3^2-1 = 8$ и имеет два делителя $M_1 = 2$, $M_2 = 4$, т.е. в данном поле существуют только двузначный и четырехзначный мультипликативные характеры.

а) $M_1 = 2$: $\psi(\alpha^0) = \exp(j2\pi\ \log_\alpha \alpha^0/2) = 1$; $\psi(\alpha) = \exp(j2\pi/2) = -1$; $\psi(\alpha^4) = \exp(j2\pi\ 4/2) = 1$; $\psi(\alpha^7) = \exp(j2\pi\ 7/2) = -1$;

б) $M_2 = 4$: $\psi(\alpha^0) = \exp(j2\pi\ 0/4) = 1$; $\psi(\alpha) = \exp(j2\pi/4) = +j$; $\psi(\alpha^4) = \exp(j2\pi\ 4/4) = 1$; $\psi(\alpha^7) = \exp(j2\pi\ 7/4) = \exp(j7\pi/2) = -j$.

На рис. 2.2 показаны мультипликативные характеры элементов группы $G_\times$: при $M_1 = 2$ характер $\psi(x)$ принимает два значения 1 и –1 (рис.2.3,а); при $M_2 = 4$ характер принимает четыре комплексных значения 1, –1, j, $-j$.

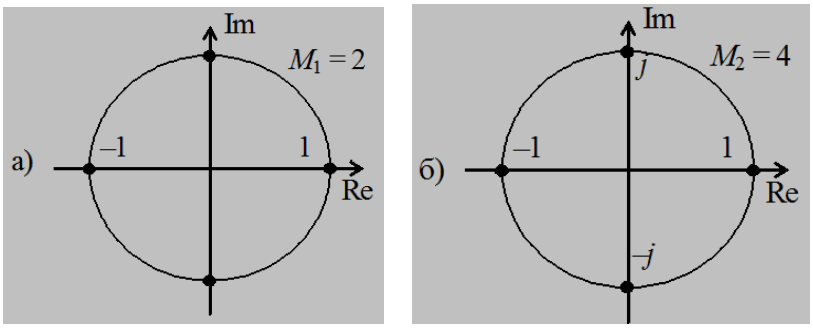

Рис.2.2. Мультипликативные характеры элементов группы $G_\times$

Решение к задаче 2.42.

а) $A_1'(x) = 11\alpha^3 x^{10} + 7\alpha^8 x^6 + 4\alpha^5 x^3 + 2\alpha x^2 + 0 = \alpha^3 x^{10} + \alpha^8 x^6$;

б) коэффициенты полинома $A_2(x)$ являются целочисленной формой представления элементов поля $GF(2^4)$; во избежание ошибок их лучше представить в степенной форме

$A_2'(x) = 11\alpha^2 x^{10} + 10\alpha^7 x^9 + 5\alpha^3 x^4 + 3\alpha^5 x^2 + 2\alpha x = \alpha^2 x^{10} + \alpha^3 x^4 + \alpha^5 x^2$.

Решение к задаче 2.43.

$A_1'(x) = 14 \bmod 5\cdot\alpha^5 x^{13} + 12\cdot 4\alpha^{17} x^{11} + 10\cdot 3\alpha^{23} x^9 + 8\alpha x^7 + 7\cdot 2\alpha^5 x^6 + 5\cdot 4\alpha x^4 + 3 +$
$+ 0 = 4\alpha^5 x^{13} + 3\alpha^{17} x^{11} + 3\alpha x^7 + 4\alpha^5 x^6 + 3.$

Список использованных источников

1. *Стародубцев В.Г., Павлов О.А.* Помехоустойчивые коды в телекоммуникационных и информационных системах. – СПб., 2003. – Вып.1. Конечные поля Галуа: элементы теории и практики. – 255 с.

2. *Френкс Л.* Теория сигналов / пер. с англ.; под ред. Д.Е. Вакмана. – М.: Сов. радио, 1974. – 152 с.

3. *Виноградов М.И.* Основы теории чисел. – М.: Наука, 1972. – 168 с.

4. *Муттер В.М.* Основы помехоустойчивой телепередачи информации. – Л.: Энергоатомиздат, 1990. – 288 с.

5. *Ипатов В.П.* Периодические дискретные сигналы с оптимальными корреляционными свойствами. – М.: Радио и связь, 1992. – 152 с.