ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ

УТВЕРЖДАЮ:
Зав. каф. РЗИ
_____ Задорин А.С.
«_____» 2006 г.

МАТЕМАТИЧЕСКИЕ ОСНОВЫ КРИПТОЛОГИИ

Курс лекций для специальностей 090103 (организация и технология защиты информации) и 090104 (комплексная защита объектов информатизации)

Разработчики:
ассистент каф. РЗИ
_____ Гецель А.В.
доц. каф. РЗИ
_____ Литвинов Р.В.

ТОМСК 2006

ОГЛАВЛЕНИЕ

Введение 4
I. Элементарные оценки сложности вычислений 7
§I.1. Числа в разных базах 7
§I.2. Число разрядов 10
§I.3. Двоичные операции. 10
§I.4. Формализация сравнения оценок сложности вычислений 14
§I.5. Полиномиальный алгоритм 19
II. ЭЛЕМЕНТЫ ТЕОРИИ ЧИСЕЛ 20
§II.1. Делимость 21
§II.2. Простые числа. 32
§II.3. Сравнения 37
§II.4. Функция Эйлера 54
§II.5. Решение сравнений первой степени, линейный конгруэнтный генератор 68
§II.6. Сравнение любой степени по простому модулю 74
§II.7. Решение систем сравнений 76
§II.8. Сравнение второй степени 78
§II.9. Решение сравнений по составному модулю 88
III. ОСНОВЫ ТЕОРИИ ГРУПП 90
§III.1. Основные понятия 90
§III.2. Группы 98
§III.3. Группы связанные с шифрами 107
§III.4. Подгруппы 111
§III.5. Приведенная система вычетов по простому модулю 120
IV. КОЛЬЦА И ПОЛЯ 127
§IV.1. Кольца 127
§IV.2. Поля 130

§IV.3. Подкольца, идеалы 133
§IV.4. Многочлены над полем 138
§IV.5. Регистры сдвига с обратной связью. Свойства периодичности ... 154
Список использованных источников 170

ВВЕДЕНИЕ

Пособие посвящено криптологии (kryptos – тайный (греч.), logos – наука (греч.)), - науке занимающейся построением и оценкой стойкости шифров (криптосистем). Обычно ее так и подразделяют на криптографию и криптографический анализ, криптография занимается построением криптосистем, а криптографический анализ – оценкой их стойкости.

Ключевым понятием данной науки является понятие криптосистемы или шифра. Существует огромное многообразие определений «шифра», и в дальнейшем мы обязательно дадим полное развернутое, сейчас же для краткости определим просто и понятно. Криптосистема (шифр) – это процесс обратимого преобразования информации с целью скрытия, на основе ключа. Обязательным атрибутом криптосистемы является ключ, если в алгоритме отсутствует ключ, о криптоалгоритме не может быть и речи. Существует несколько смежных отраслей близких к криптологии. Например, сокрытием данных в пределах некоторого набора данных занимается стеганография, преобразованием информации в вид удобный для передачи занимается теория кодирования, а так же существует теория сжатия данных, занимающаяся преобразованием данных с целью уменьшения объема. Как мы видим все эти области знаний используют преобразование информации, однако не в одной из них нет ключа, на основе которого происходит преобразование. Наличие ключа – явный признак, по которому можно выделить криптологию от ряда смежных наук.

Необходимость в криптологии возникло когда у одного человека появились знания, дающие ему технологические, тактические или иные преимущества перед другими. Первые криптосистемы были разработаны необыкновенно давно и авторами их были люди стоящие у власти или близкие к ней, такие как цезари, королевские особы, правители и пр. Сейчас их разра-

ботки кажутся по детски простыми и наивными, однако на тот момент этого было достаточно для скрытия важных сведений. Для наивной криптографии (до начала XVI в.) присущи простейшие примитивные преобразования. Одним из первых шифров этой эпохи принято считать шифр Цезаря, его смысл состоял в замене каждой буквы на букву, отстоящую на несколько позиций от заданной. Еще одним представителем криптосистем являлся квадрат Полибия. Квадрат имел размер 5X5 и заполнялся всеми буквами английского алфавита в некотором порядке, при шифровании каждая буква заменялась на находящуюся под ней букву.

Следующей эпохой – эпоха формальной криптографии (конец XV – начало XX). Она связана с бурным развитием науки, начавшимся в эпоху Возрождения в европейских странах. В этот период появились первые стойкие для ручного (не машинного) криптоанализа шифры и первые научные работы посвященные предмету. Важным открытием в этом этапе стало изобретение сделанное Леоном Батистом Альберти. Он предложил шифр, впоследствии названный шифром Виженера. В течении этой эпохи были написаны несколько важных для науки работ: «Трактат о шифре» Л.Б. Альберти, «Полиграфия» Иоганна Трисемуса. А так же сформулировано важное правило, названное впоследствии основным правилом криптографии (правило Керкхгоффа): «Секретность шифра должна основываться на стойкости ключа, а не секретности шифра». И на конец этой эпохи приходится изобретение механических роторных машин, на основе которых была разработана немецкая роторная машина «Энигма».

Эпоха научной криптографии (30-е – 60-е г. XX в) подвела математическую базу под науку, в основание было положены разделы теории чисел, теории вероятности и математической статистики, общей алгебры, теории алгоритмов, теории информации. Важной работой была работа Клода Шеннона «Теория связи в секретных системах», в ней было введено понятие совершенно стойкого шифра.

Следующая эпоха – эпоха компьютерной криптологии (с 70-х г.г. XX в.) стала возможной благодаря бурному развитию вычислительных средств. В течении этого периода было разработано большинство современных криптосистем DES (американский стандарт передачи данных), отечественных ГОСТ 28147-89. Разработано множество криптоатак, большинство из которых, стали возможными благодаря использованию вычислительных систем. А так же появилось важное направление – несимметричная криптология, благодаря которой стали возможными протоколы цифровой подписи, разделения секрета и пр.

Развитие науки можно проследить на основе эволюции ключа, используемого при шифровании. В донаучной криптологии ключ представлял из себя величину сдвига, матрицу подстановки, либо слово. В период после научной криптологии для генерации ключа используется специальные приложения. Например, в современной криптосистеме PGP используется 512, 1024, 2048 и т.д. битные ключи.

Задача данного пособия - дать студентам базовые теоретические знания, ту самую основу, которая была сформирована в эпоху научной криптологии.

Основное содержание курса составляют: теория чисел, теория групп, теория колец и полей.

Задача курса дать базовые знания о математическом аппарате, также ознакомить с основными криптографическими алгоритмами. Содержание составляют базовые понятия выше перечисленных разделов и их основные свойства. Сведений изложенных в учебном пособии достаточно для того чтобы программно реализовать простейшие криптоалгоримы такие как нахождение обратных чисел, генерация чисел, проверка числа на простоту, реализация простейших криптосистем.

I. ЭЛЕМЕНТАРНЫЕ ОЦЕНКИ СЛОЖНОСТИ ВЫЧИСЛЕНИЙ

§I.1. ЧИСЛА В РАЗНЫХ БАЗАХ

Разложение неотрицательного целого числа n по основанию (базе) b представляет собой обозначение для n вида

$$n \leftrightarrow (d_{k-1}d_{k-2}...d_1d_0)_b, \tag{1.1}$$

где d_j – цифры, т.е. символы целых чисел от $d = 0$ до $d = b - 1$. Эта запись означает, что

$$n = d_{k-1}b^{k-1} + d_{k-2}b^{k-2} + ... + d_1b + d_0 = \sum_{j=1}^{k} d_{k-j}b^{k-j} \tag{1.2}$$

Если цифра первого разряда отлична от нуля, то число n называют k-разрядным b-ичным числом. Любое целое число от b^{k-1} до $b^k - 1$ является k-разрядным по основанию b. Как обычно, будем опускать скобки и индекс $(...)_b$ в случае десятичной системы счисления ($b = 10$) и в тех случаях, когда основание системы счисления ясно из контекста, особенно в случае двоичной системы ($b = 2$).

Дробные числа x также можно разлагать по любому основанию, т. е. представлять в виде

$$x \leftrightarrow (d_{k-1}d_{k-2}...d_1d_0, d_{-1}d_{-2}...)_b, \tag{1.3}$$

При $b > 10$ принято использовать буквы для выражения цифр, больших девя-

ти. Можно вообще использовать буквы вместо цифр.

Поскольку иногда удобно пользоваться системами, отличными от десятичной, приходится производить арифметические операции по произвольному основанию и переходить от одного основания к другому. Продемонстрируем это на нескольких примерах.

ПРИМЕР 1.

1.1.

$(11001001)_2 = 201$.

1.2.

При $b = 26$ будем использовать буквы латинского алфавита $A - Z$ для записи цифр от 0 до 25, соответственно. Тогда $(BAD)_{26} = 679$, тогда как $(B,AD)_{26} = 1\frac{3}{676}$.

ПРИМЕР 2.

Задание

Умножить 160 на 199 в системе счисления по основанию 7.

Решение:

Для решения переведем сначала числа в семеричную систему исчисления $160 = (316)_7$ и $316 = (403)_7$. Затем воспользуемся обычным правилом умножения в столбик.

$$\begin{array}{r} 316 \\ \times\ 403 \\ \hline 1254 \\ 16030 \\ \hline 161554 \end{array}$$

ПРИМЕР 3.

Задание

Разделить $(11001001)_2$ на $(100111)_2$ и $(HAPPY)_{26}$ на $(SAD)_{26}$.

Решение:

11001001 | 100111	HAPPY | SAD
100111 | 101	GYBE | KD
101101	COLY
100111	CCAJ
110 (ост)	MLP (ост)

ПРИМЕР 4.

Задание

Выразить 106 в системах счисления по основаниям 2, 7 и 26 (в последнем случае использовать буквенную запись).

Решение.

Чтобы разложить число n по основанию b, надо сначала получить младший разряд, разделив n на b и взять остаток от деления. Потом n заменяется частным от деления, описанный процесс повторяется и дает второй от конца знак разложения и т. д. В данном случае получаем

$106 = (11110100001001000000)_2 = (11333311)_7 = (CEXHO)_{26}$.

ПРИМЕР 5.

Задание

Выразить π = 3,1415926 ... в двоичной системе счисления (выписывая 15 цифр после запятой).

Решение.

Сначала представляется целая часть. Потом дробная часть умножается на основание b. Целая часть полученного числа дает d_{-1}, а к его дробной части применяется та же процедура, что последовательно дает d_{-2}, d_{-3}....Таким способом получаем:

$3,1415926... = (11,001001000011111...)_2 = (D, DRS ...)_{26}$.

§I.2. ЧИСЛО РАЗРЯДОВ.

Из формулы (1.1) и (1.2) следует, что целое число, удовлетворяющее неравенствам

$$b^{k-1} \le n < b^k \ ,$$

имеет k разрядов по основанию b. Логарифмируя последнее соотношение и используя функцию $[n]$ взятия целого от числа n получим для числа разрядов k следующее соотношение

$$k = \left[\log_b n\right] + 1 = \left[\frac{\log_2 n}{\log_2 b}\right] + 1 = \left[\frac{\ln n}{\ln b}\right] + 1 . \qquad (1.4)$$

§I.3. ДВОИЧНЫЕ ОПЕРАЦИИ.

Начнем с очень простой арифметической задачи сложения двух двоичных целых чисел, например,

```
1 1 1 1 - (перенос)
  1111000
+ 0011110
 10010110
```

Предположим, что оба числа имеют длину в k бит (слово «бит» является сокращением выражения «binary digit»). Если запись одного из чисел короче, ее можно дополнить нужным числом нулей слева. Хотя в примере рассматриваются маленькие целые (складываются $120 \leftrightarrow (1111000)_2$ и $30 \leftrightarrow (0011110)_2$), следует иметь в виду, что число k может быть очень большим, скажем, $500 \leftrightarrow (111110100)_2$ или $1000 \leftrightarrow (1111101000)_2$.

Детально проанализируем всю процедуру сложения. При сложении необходимо k раз повторить следующие шаги:

1. Посмотреть на верхний и нижний биты, а также проверить, имеется ли

перенос единицы от сложения младших разрядов.

2. Если оба бита нулевые, а переноса нет, то в данном разряде суммы записываем нуль и двигаемся дальше.
3. Если либо а) оба бита нулевые и есть перенос, либо б) один бит – нуль, другой – единица и переноса нет, то записываем единицу и двигаемся дальше.
4. Если либо а) один бит – нуль, другой – единица и есть перенос, либо б) оба бита – единицы и переноса нет, то записываем нуль в данный разряд, записываем единицу переносов в следующий столбец и двигаемся дальше.
5. Если оба бита — единицы и есть перенос, то в данном разряде суммы записываем единицу, записываем единицу переносов в следующий столбец и двигаемся дальше.

Однократное выполнение этих шагов называется двоичной (битовой) операцией. Очевидно, что *сложение* двух k-разрядных двоичных чисел требует k двоичных операций.

Мы увидим ниже, что и более сложные задачи тоже могут быть разбиты на двоичные операции. Время, которое расходует компьютер на решение задачи, по сути дела пропорционально числу двоичных операций. Конечно, константа пропорциональности – число наносекунд, расходуемых на одну двоичную операцию, – зависит от вида компьютера. (Сказанное является упрощением, так как это время может зависеть также от «технических» факторов, например, времени доступа к памяти.) Когда мы говорим об оценке времени работы, подразумевается оценка числа двоичных операций. В этих оценках мы будем пренебрегать временем, расходуемым на запись информации или на логические шаги, отличные от двоичных операций. На практике основное время занимает выполнение именно двоичных операций.

Оценка числа N двоичных операций процесса умножения в столбик k-разрядного двоичного числа n на l-разрядное двоичное число m показывает

(доказательство в курсе практических занятий), что

$$\begin{array}{l} N < kl < k^2 (\text{если } n > m) \\ N < l^2 (\text{если } m > n) \end{array} \qquad (1.5)$$

Формула (1.4) позволяет переписать эту оценку в терминах самих чисел n и m в виде:

$$N < \left(\frac{\ln n}{\ln 2} + 1\right)\left(\frac{\ln m}{\ln 2} + 1\right). \qquad (1.6)$$

В случае больших чисел n и m, таких что $\ln n >> 1$ и $\ln m >> 1$ последняя формула упрощается

$$\begin{array}{l} N < \ln n \ln m < \ln^2 n \,(\text{если } n > m), \\ N < \ln^2 m \,(\text{если } m > n) \end{array} . \qquad (1.7)$$

Оценка числа N двоичных операций нахождения факториала $n!$ показывает , что

$$\begin{array}{l} N < (n-2)n(\log_2 n + 1)^2 \\ N < n^2 \log_2^2 n \;\; (\text{если } \log_2 n >> 1) \end{array} . \qquad (1.8)$$

Оценка верхней границы числа N двоичных операций, необходимых для умножения многочлена $\sum a_i x^i$ степени не выше n_1 на многочлен $\sum b_j x^j$ степени не выше n_2 с положительными целыми коэффициентами не превосходящими m приводит к следующему соотношениям:

$$N < (n_1 + n_2 + 1)\left((n_2 + 1)(\log_2 m + 1)^2 + n_2\left(\log_2\left(n_2 m^2\right) + 1\right)\right),$$
$$N < \frac{n_2(n_1 + n_2)}{\ln 2}\left(\frac{\ln^2 m}{\ln 2} + \ln n_2 + 2\ln m\right). \qquad (1.9)$$

Положим $n = n_1 \geq n_2$, и пусть $m \geq 16$ и $m \geq \sqrt{n_2}$ (что обычно выполняется на практике). Тогда последнее выражение можно упростить до

$$N < 4n^2 \log_2^2(n_2 m) \qquad (1.10)$$

Этот пример показывает, что в общем случае нет единого «правильного ответа» на вопрос о нахождении границы для времени решения задачи. Можно искать границу как достаточно простую функцию от исходных данных (в рассмотренном случае это n_1, n_2 и m), которая для большинства исходных данных дает оценку, по порядку более или менее близкую к числу реально выполняемых двоичных операций. Поэтому в рассмотренном случае числа операций при умножении многочленов нет смысла заменять нашу оценку оценкой $4n^2m$, так как при больших n она на много порядков больше реального числа операций.

До сих пор мы имели дело со сложением и умножением целых чисел. Две другие арифметические операции – вычитание и деление – имеют те же самые оценки временной сложности, что сложение и умножение соответственно. Более точно, для описания вычитания надо расширить круг двоичных операций, включив в него операцию вычитания нуля или единицы из других нуля или единицы, возможно, с займом единицы из старшего разряда.

Анализируя деление в двоичной системе, будем использовать следующее рассуждение. Пусть количество разрядов делимого k больше, чем количество разрядов l в делителя (т.е. $k > l$, если $k < l$, то деление тривиально, т. е. частное равно нулю, а все делимое образует остаток). Нахождение частного и остатка требует самое большее $k - l + 1$ вычитаний. Каждое вычитание тре-

бует l или $l + 1$ двоичных операций, но в последнем случае в самом левом разряде разности будет стоять нуль, поэтому можно опустить одну двоичную операцию (считая, что это скорее операция «по учету данных», а не вычисление). Подобным образом мы игнорируем и другие технические детали, например, сравнение двоичных целых чисел (при определении минимального числа разрядов делимого, которые образуют число, большее делителя), снос разрядов и т.п. Таким образом, наша оценка есть просто $(k - l + 1)l$, что не больше kl.

Оценка верхней границы числа N двоичных операций, необходимых для вычисления биномиального коэффициента $\binom{n}{m} = \binom{n}{n-m}$ дает следующее соотношение

$$N < 2(m-1)m(\lceil \log_2 n \rceil + 1)^2 \ , \qquad (1.11)$$

что при больших числах m и n приблизительно равно $N < 2m^2(\log_2 n)^2$.

§I.4. ФОРМАЛИЗАЦИЯ СРАВНЕНИЯ ОЦЕНОК СЛОЖНОСТИ ВЫЧИСЛЕНИЙ

Введем обозначение для краткой записи оценок сложности вычислений, так называемое **O-«большое»**. Пусть $f(n)$ и $g(n)$ — функции положительного целочисленного аргумента, принимающие положительные (не обязательно целые) значения при всех n. Скажем, что $f(n) = O(g(n))$ (или просто $f = O(g)$), если существует такая константа C такая, что $f(n)$ всегда меньше $Cg(n)$. Например, $2n^2 + 3n - 3 = O(n^2)$ (действительно, нетрудно доказать, что левая часть меньше $3n^2$).

Обозначение O-большое используется и в более общей ситуации. Дадим этому обозначению более широкое определение. Рассмотрим f и g как функции нескольких переменных n_j и не будем обращать внимание на соотношение между ними при небольших значениях аргументов n_j. Так же, как

это делается в теории пределов в анализе, будем рассматривать лишь большие значения n_j.

Определение. Пусть $f(n_1, n_2,..., n_r)$ и $g(n_1, n_2,..., n_r)$ – две функции, определенные на наборах из r положительных целых чисел. Предположим, что существуют такие константы B и C, что, когда все n_j больше B, обе функции положительны и $f(n_1, n_2,..., n_r) < Cg(n_1, n_2,..., n_r)$. В этом случае говорим, что функция f ограничена функцией g, и пишем $f = O(g)$.

Заметим, что равенство в обозначении $f = O(g)$ следует, скорее, понимать как неравенство “<” , а О-большое – как некоторую мультипликативную константу.

ПРИМЕР 6.

6.1

Пусть $f(n)$ – произвольный многочлен степени d с положительным старшим коэффициентом. Тогда, как легко показать, $f(n) = O(n^d)$. В более общем случае можно показать, что $f = O(g)$, если $f(n)/g(n)$ имеет конечный предел при $n \to \infty$.

6.2

Если ε – сколь угодно малое положительное число, можно показать, что $\ln n = O\left(n^{\varepsilon}\right)$ (т.е. при больших n функция ln меньше любой степенной, сколь малой ни была бы степень). Это следует из равенства $\lim_{n\to\infty}\left(\ln n / n^{c}\right) = 0$, которое доказывается с помощью правила Лопиталя.

6.3

Если $f(n)$ обозначает число k двоичных разрядов числа n, то, как следует из приведенных выше формул для k, $f(n) = O(\ln n)$.Заметим, что такое же соот-

ношение выполнено, если $f(n)$ число разрядов в разложении n по произвольному фиксированному основанию b. С другой стороны, если основание b не фиксировано, а может расти, и $f(n,b)$ – число разрядов в записи по основанию b, то $f(n,b) = O(\ln n / \lg b)$

6.4

Имеем $N(nm) = O(\ln n \ln m)$, где в левой части стоит число двоичных операций, требующихся для умножения n на m.

6.5

$$N(n!) = O(n(\ln n)^2)$$

6.6

$$N\left(\sum a_i x^i \sum b_j x^j\right) = O\left(n_1 n_2 \left(\ln^2 m + \ln(\min(n_1; n_2))\right)\right)$$

Функции $f(n)$ и $f(n_1, n_2,..., n_r)$ часто отождествляются с временем (сложностью вычислений), которое требуется для решения некоторой арифметической задачи с целым числом n или с набором целых чисел $n_1, n_2,..., n_r$ в качестве исходных данных. Удобно получать оценки сложности вычислений в виде достаточно простых функций $g(n)$. При этом желательно, чтобы функции $g(n)$ не давали чрезмерно завышенного представления о времени решения задач (хотя с чисто математической точки зрения замена функции $g(n)$ в соотношении $f = O(g)$ любой большей функцией корректна).

Образно говоря, соотношение $f(n) = O(n)$ показывает, что функция f растет приблизительно как d-я степень аргумента. Например, если $d = 3$, то оно говорит нам, что удвоение аргумента приведет к увеличению функции приблизительно в 8 раз. Соотношение $f(n) = O(\ln^d n)$ показывает, что функция возрастает приблизительно как d-я степень числа двоичных разрядов в n. Это так, потому что с точностью до мультипликативной константы число бит равно приблизительно $\ln n$ (а именно, $\ln n / \ln 2 = 1{,}4427 \ln n$). Так, например, если

$f(n) = O(\ln n)$, то удвоение числа бит в n (что гораздо сильнее увеличивает аргумент, нежели его удвоение) приводит к увеличению $f(n)$ приблизительно в 8 раз.

Заметим, что запись $f(n) = O(1)$ означает, что функция f ограничена некоторой константой.

Число двоичных операций при умножении двух чисел приблизительно одинакового размера в случае простого способа умножения «столбиком» можно оценить по формуле (1.5). Следует заметить, что было предпринято много усилий по повышению скорости умножения двух k-разрядных двоичных чисел при больших k. Используя специальные приемы, много более сложные, чем обычный школьный способ умножения, математики смогли придумать процедуру умножения двух целых чисел из k бит, требующую всего $O(k\ln k\ln\ln k)$ двоичных операций . Это лучше, чем $O(k^2)$, и даже лучше, чем $O(k^{1+\varepsilon})$ при любом сколь угодно малом $\varepsilon > 0$. Однако дальше будем пользоваться только приведенными выше грубыми оценками для времени (числа двоичных операций), необходимого для умножения.

В общем случае, когда оценивается число двоичных операций, требующихся для решения какой-либо задачи, сначала надо определить и выписать подробную процедуру решения задачи. Конкретная *пошаговая процедура* выполнения вычислений называется *алгоритмом*. Конечно, может существовать много разных алгоритмов, выполняющих одну и ту же работу.Можно воспользоваться тем из них, который попроще в записи, или тем, который быстрее работает, или выбрать какой-то компромисс между простотой и быстродействием. Использованный выше алгоритм умножения n на m далек от самого быстрого из известных. Но вместе с этим он много быстрее метода повторного сложения (m-кратного сложения числа n с собой).

ПРИМЕР 7.

Задание

Оценить число двоичных операций (время), требующихся для перевода числа из k бит в десятичную систему счисления.

Решение.

Пусть n – целое из k бит, записанное в двоичной системе счисления. Алгоритм перевода следующий. Разделим n на $10 = (1010)_2$. Остаток от деления – который является одним из чисел 0, 1, 10, 11, 100, 101, 110, 111, 1000 или 1001 – даст содержимое d_0 разряда единиц. Частное от деления возьмем вместо n, поделим на $(1010)_2$ и возьмем остаток от этого деления в качестве d_1, а частное – в качестве делимого при следующем делении на $(1010)_2$. Это процесс должен повторяться столько раз, сколько десятичных разрядов содержится в числе n, т.е. $[\ln n/\ln 10]+1 = O(k)$. Тогда процесс будет завершен. (Наши записи мы могли вести и в десятичной системе, используя более привычные обозначения для остатков 0,1,2,3,... ,9 вместо 0,1,10,11,..., 1001.) Как много двоичных операций будет сделано? Мы сделали $O(k)$ делений, каждое из них требовало $O(4k)$ операций (делимое содержит не более k бит, а делитель $(1010)_2$ – 4 бита). Но $O(4k)$ эквивалентно $O(k)$ (постоянный множитель несуществен в обозначении «О-болшое»). Поэтому общее число двоичных операций равно $O(k)\cdot O(k) = O(k^2)$. Если желательно выразить оценку в терминах n, а не k, то, используя равенство $k = O(\ln n)$, можно записать

N(перевод числа n из двоичной в десятичную систему счисления) $= O(\ln n)$(1.12)

ПРИМЕР 8.

Задание

Оценить число двоичных операций (время), требующихся для перевода числа n из k бит в систему счисления по основанию b, которое может быть очень большим.

Решение.

Используя алгоритм примера 7 (только делим теперь на число b из l бит), по-

лучаем, что каждое деление выполняется дольше (если l велико) и требует $O(k/l)$ двоичных операций. А сколько раз придется делить? Следует заметить, что число разрядов при записи n в 6-ичной системе равно $O(k/l)$ (см. пример 6.3). Поэтому общее число двоичных операций во всех делениях равно $O(k/l) - O(kl) = O(k^2)$. Это тот же ответ, что и в примере 7. Значит, наша оценка для времени перевода числа в новую систему счисления не зависит от основания системы (сколь бы большим оно ни было). Это так, поскольку увеличение времени для определения содержимого каждого разряда компенсируется уменьшением числа этих разрядов.

ПРИМЕР 12.

Задание

Выразить при помощи «О-большого» время, требующееся для вычисления $n!$, $\binom{n}{m} = \binom{n}{n-m}$.

Решение

Используя формулу (1.8) получим $O(n^2 \log^2 n)$.

Используя формулу (1.11) получим $O(m^2 \log^2 n)$

§I.5. ПОЛИНОМИАЛЬНЫЙ АЛГОРИТМ

В завершение дадим одно определение, являющееся фундаментальным в вычислительных науках и в теории алгоритмов.

Алгоритм для проведения вычислений, определяющихся целыми числами $n_1, n_2, \ldots, n_r$ из $k_1, k_2, \ldots, k_r$ бит, соответственно, называется полиномиальным по времени алгоритмом, если существуют такие целые числа $d_1, d_2, \ldots, d_r$, что число двоичных операций при работе этого алгоритма равно

$$N_{polynominal} = O\left(k_1^{d_1} k_r^{d_r} \ldots k_r^{d_r}\right). \qquad (1.12)$$

Таким образом, обычные арифметические операции сложение (+), вычитание(–), умножение (·), деление (/) дают примеры полиномиальных по времени алгоритмов. Еще один пример – перевод чисел из одной системы счисления в другую. С другой стороны, вычисление $n!$ не является такой операцией. (Однако, если требуется найти лишь заданное число значащих цифр, например, первые 1000 двоичных разрядов, то можно найти $n!$ за полиномиальное время при помощи формулы Стирлинга .)

II. ЭЛЕМЕНТЫ ТЕОРИИ ЧИСЕЛ

Теория чисел — раздел математики, занимающийся изучением чисел непосредственно как таковых, их свойств и поведения в различных ситуациях. Теория чисел берет свое начало в глубокой древности. Среди основоположников сей науки можно выделить Евклида, Диофанта, Аристотеля и пр.

На протяжении всего учебного пособия мы будем работать на множестве целых чисел и только на нем. Если мы где-то будем говорить «Возьмем некоторое число…», всегда будет подразумеваться, что число целое, полученные результаты тоже целые числа, вся арифметика в данном пособии целочисленная. Отступим от данного правила мы лишь несколько раз когда будем говорить о вероятности, но эти ситуации мы строго обозначим.

Множество целых чисел будем обозначать $\mathbf{Z} = \{\ldots -3, -2, -1, 0, 1, 2, 3, \ldots\}$,

Множества целых чисел отличных от нуля $\mathbf{Z^*} = \{\ldots -3, -2, -1, 1, 2, 3, \ldots\} = \mathbf{Z} - \{0\}$.

По ходу доказательств, и в формулировках определений для упрощения записи, мы будем использовать логические и математические символы:

$\exists$ - существует;

$\exists!$ - существует единственный;

$\in,\notin$ - принадлежит и не принадлежит соответственно;

$\wedge$ - обозначает логическое “*и*”;

$\vee$ - логическое “*или*”;

$\neg$ - логическое “*не*”.

Например,

$a=b \wedge b=c$ – читается «a равно b и b равно c»

$a=b \wedge \neg b=c$ – читается «a равно b и b не равно c»

§II.1. ДЕЛИМОСТЬ

Понятие делимости знакомо каждому еще с начальной школы, сформулируем в очередной раз его определение [1].

Определение: Пусть $a,b \in \mathbf{Z}$, говорят, что a делит b и записывают $a|b$, если $\exists c$ такое, что $b=ac$. Число a будем называть делителем b, а b кратно a.

Примеры

$-7|21$ т. к. $\exists(-3)$, такое что $21=(-7)\cdot(-3)$

$17|0$ т. к. $\exists 0$, такое что $0 = 113*0\cdot$

Отметим, что для $\forall a \in \mathbf{Z}^*$ $a|0$

Свойства делимости

1) Любое отличное от нуля число делит себя, или математическим языком $\forall a \in \mathbf{Z^*}\ a|a$. Справедливость данного свойства обосновывается тем, что $a=1\cdot a$, то есть, в контексте нашего определения деления - существует такое число "*1*", что $a=1\cdot a$.

2) Единица делит любое число $\forall a \in \mathbf{Z}\ 1|a$, т.к. $a=1\cdot a$

3) Делимость не зависит от знака, или $a|b \Rightarrow -a|b$. Обосновать свойство можно следующим $b=a\cdot c=(-a)\cdot(-c)$.

4) Транзитивность, определим его математическим языком $a|b \wedge b|c \Rightarrow a|c$.

   Докажем: $a|b \Rightarrow b=ad$, аналогично $b|c \Rightarrow c=be$, отсюда $c=be=(ad)e=a(de) \Rightarrow a|c$.

5) $a|b \wedge a|c \Rightarrow a|(bx+cy)$

   $$\left.\begin{array}{l} a|b \Rightarrow b=ae \\ a|c \Rightarrow c=ad \end{array}\right\} \Rightarrow (bx+cy) = (aex+ady) = a(ex+dy) \Rightarrow a|a(ex+dy)$$

6) $a|b \wedge b|a \Rightarrow a=\pm b$

   $$\left.\begin{array}{l} a|b \Rightarrow b=ac \\ b|a \Rightarrow a=be \end{array}\right\} \Rightarrow b=ac=(be)c=b(ec) \Rightarrow ec=1 \Rightarrow c=e=\pm 1 \Rightarrow a=\pm b$$

Для любых двух чисел a,b нельзя однозначно сказать, что $a \mid b$ или $b \mid a$, поэтому определим понятие деления с остатком [1,3].

Теорема (о делении с остатком)

Всякое число a можно представить единственным образом через положительное целое b ($b>0$) в виде

$$a = bq + r, \quad \text{где } 0 \le r < b$$

q называется неполным частным, его можно записать как $q = a \text{ div } b$, r - оста-

ток от деления a на b($r = a \bmod b$).

Доказательство

1) Докажем существование представления.

Выберем q из условия

$$bq \le a < b(q + 1); \quad r = a - bq$$

преобразуем

$$0 \le a - bq < b; \quad a - bq = r$$

получили

$$a = bq + r; \quad 0 \le r < b$$

2) Докажем единственность подобного представления от противного. Предположим, что a представляется через b двумя способами:

$a = bq_1 + r_1 = bq_2 + r_2$

Преобразуем

$bq_1 - bq_2 = r_2 - r_1$

$b(q_1 - q_2) = r_2 - r_1 \Rightarrow b \mid r_2 - r_1$ (1)

Из того, что $0 \le r_1 < b$ $0 \le r_2 < b \Rightarrow |r_2 - r_1| < b$. (2)

Из (1) и (2) $\Rightarrow r_2 = r_1 \quad \Rightarrow b_1 = b_2$.■

Примеры

Представим *17* через *3*

$17 = 3 \cdot 5 + 2$, здесь *5* – неполное частное, а *2* – остаток.

Представим *–25* через *3*

$-25 = 3 \cdot (-8) + 1$

Представим *–16* через *3*

$-16 = 3\,(-6) + 2$.

Определение: Число $d \in \mathbf{Z}$, делящее одновременно числа $a_1, a_2, \ldots a_n \in \mathbf{Z}$, называется общим делителем этих чисел. Наибольшее d с таким свойством

называется ***наибольшим общим делителем*** и обозначается НОД($a_1, a_2, \ldots a_n$).

В спец литературе зачастую для НОД используется обозначение ($a_1, a_2, \ldots a_n$), однако мы будем использовать интуитивно более понятное НОД($a_1, a_2, \ldots a_n$).

Примеры

НОД (*72*;*15*)=*3*

НОД (*100*; *20*)=*20*

НОД (*113*; *15*)=*1*

Если НОД($a_1, a_2, \ldots a_n$) =*1*, то числа $a_1, a_2, \ldots a_n$ называются ***взаимно простыми числами***, если же НОД (a_i, a_j) =*1* $\forall j \neq i$, то a_1, a_2, $\ldots a_n$ - ***попарно простые числа***. Очевидно, попарно простые числа окажутся и взаимно простыми. Из попарно простоты следует взаимная простота, но из взаимной простоты не следует попарно простота.

Пример

Числа {*3*, *6*, *7*, *8*} взаимно просты, т.к. НОД(*3*, *6*, *7*, *8*)=*1*, но попарно не просты, поскольку НОД(*3*, *6*)=*3* и НОД(*6*, *8*)=*2*.

Совокупность чисел {*3*, *5*, *8*} попарно просты, т.к. НОД(*3*, *5*)=*1*, НОД(*3*, *8*)=*1* и НОД(*5*, *8*)=*1*, и, обладая попарно простотой они обладают и взаимно простотой т.е. НОД(*3*, *5*, *8*)=*1*.

Свойства НОД

В действительности можно было привести порядка десяти свойств НОД, однако востребованными окажутся лишь несколько, ими и ограничимся.

1) Для любых целых чисел a и k, очевидно, справедливо: НОД(a, ka) = a.
Иначе это свойство можно сформулировать следующим образом:
Если $a|b \Rightarrow$ НОД(a, b) = a.

2) Если $a = bq + c$, то совокупность общих делителей a и b совпадает с совокупностью общих делителей b и c, в частности, НОД(a, b)=НОД(b, a mod b) [1].

Доказательство

Пусть d – общий делитель a и b ($d|a$, $d|b$), тогда $d|c$, поскольку $a = bq + c$.

Обратно, d – общий делитель b и c ($d|c$, $d|b$), тогда $d|a$.

Алгоритм Евклида

Найти НОД для двух небольших чисел несложно, однако попробуйте найти НОД для *141128* и *77349*. Решение данной задачи впервые было сформировано во времена Птолемея I известным древнегреческим математиком Евклидом еще в IX веке.

Евклид – древнегреческий ученый математик [10], преподаватель, автор первых математических трактатов. Исторические сведения о нем крайне скудны. Известно, что он родом из Афин, был учеником Платона. Научная деятельность Евклида протекала в Александрии (3 в. до н. э.), и ее расцвет приходится на время царствования в Египте Птолемея I (306-283 г. до н.э.).

Основным трудом Евклида является книга «Начал» (Stoichéia, буквально – азбука, элементы; переносное значение - основные начала). Книга состоит из 15 глав (разделов), 13 из которых приписывают перу Евклида. Остальные два были написаны несколько позже последователями.

Евклид должен был быть моложе Архимеда, который ссылался на «Начала». Преподавал он, скорее всего, четыре науки, которые, по мнению Платона, должны предшествовать занятиям философией: арифметику, геометрию, теорию гармонии, астрономию. Кроме “Начал” до нас дошли книги Евклида, посвящённые гармонии и астрономии.

Что касается места Евклида в науке, то оно определяется не столько собственными его научными исследованиями, сколько педагогическими заслугами. Евклиду приписывается несколько теорем и новых доказательств, но их значение не может быть сравнимо с достижениями великих греческих геометров: Фалеса и Пифагора, Евдокса и Теэтета. Величайшая заслуга Евклида в том, что он подвёл итог построению геометрии и придал изложению столь совершенную форму, что на 2000 лет “Начала” стали энциклопедией геометрии.

В [9] приводится известный анекдот, согласно которому Птолемей задал Евклиду вопрос: "Нет ли в геометрии более краткого пути, чем тот, который изложен в "Началах"?" На что Евклид ответил, что в геометрии не существует царской дороги.

Осталось только добавить, что книга начал перетерпела более 500 переизданий на всех языках мира.

Алгоритм Евклида или ***алгоритм нахождения НОД*** **(*a, b*)** основан на том факте, что НОД(a, b)=НОД(b, a mod b). Современная буквенная запись алгоритма имеет следующий вид [1,3,8]

$$a = bq_1 + r_1 \qquad 0 < r_1 < b$$
$$b = r_1 q_2 + r_2 \qquad 0 < r_2 < r_1$$
$$r_1 = r_2 q_3 + r_3 \qquad 0 < r_3 < r_2$$
$$r_2 = r_3 q_4 + r_4 \qquad 0 < r_4 < r_3$$

$$r_{n-3} = r_{n-2}\,q_{n-1} + r_{n-1} \quad 0 < r_{n-1} < r_{n-2}$$
$$r_{n-2} = r_{n-1}\,q_n + r_n \quad 0 < r_n < r_{n-1}$$
$$r_{n-1} = r_n\,q_{n+1} \quad r_{n+1} = 0$$

$$r_n = \text{НОД}\,(a,b)$$

Доказательство

2 св. НОД 2 св. НОД 2 св. НОД 1 св. НОД

НОД(a, b) = НОД (b, r_1) = НОД (r_1, r_2) =…= НОД (r_{n-1}, r_n) = r_n.

Сходимость алгоритма следует из того факта, что $0 < r_n < r_{n-1} < \ldots < r_3 < r_2 < r_1 < b$.

Примеры:

1) Найдем НОД(*57*, *15*)

57 = 15·3 + 12

15 = 12·1 + 3

12 = 3·4 + 0

Ответ: НОД(*57*, *15*) = *3*.

2) Найдем НОД(*141128*, *77349*)

141128 = 77349·1 + 63779

77349 = 63779·1 + 13570

63779 = 13570·4 + 9499

13570 = 9499·1 + 4071

9499 = 4071·2 + 1357

4071 = 135·3

Ответ: НОД(*141128*, *77349*) = *1357*.

Расширенный алгоритм Евклида

Расширенный алгоритм Евклида [1,3,8] помимо d=НОД(a, b) позволяет найти числа x и y такие, что $d=bx+ay$. Расширенный алгоритм Евклида имеет следующую символьную запись

1) Сперва по алгоритму Евклида в чистом виде находим d=НОД(a, b)

$$a = bq_1 + r_1$$
$$b = r_1 q_2 + r_2$$
$$r_1 = r_2 q_3 + r_3$$
$$\dots$$
$$r_{n-3} = r_{n-2} q_{n-1} + r_{n-1}$$
$$r_{n-2} = r_{n-1} q_n + r_n$$
$$r_{n-1} = r_n q_{n+1}$$
$$r_n = d = \text{НОД}(a, b)$$

2) Далее движемся в обратном направлении

$$d = r_n = r_{n-2} - r_{n-1} \cdot q_n = r_{n-2} - (r_{n-3} - r_{n-2} \cdot q_{n-1})\, q_n = \dots = a \cdot x + b \cdot y.$$

Чтобы облегчить дальнейшую работу договоримся, что $a>b$.

Проиллюстрируем расширенный алгоритм на примерах.

Примеры

1) Проделаем расширенный алгоритм Евклида для чисел *274* и *42*, то есть найдем такие числа x и y, что $d = a \cdot x + b \cdot y$.

1.1) $274 = 42 \cdot 6 + 22$

$42 = 22 \cdot 1 + 20$

$22 = 20 \cdot 1 + 2$

$20 = 2 \cdot 10$

d=НОД(274,22)

1.2) $2 = 22 - 20 = 22 - (42 - 22) = 22 \cdot 2 - 42 = (274 - 42 \cdot 6)2 - 42 = 274 \cdot 2 - 42 \cdot 13$

Искомое представление: $2 = 274 \cdot 2 - 42 \cdot 13$. И $x = 2$, $y = -13$.

2) Проделать расширенный алгоритм Евклида для чисел 123456 и 543

2.1) $123456 = 543 \cdot 227 + 195$

$543 = 195 \cdot 2 + 153$

$195 = 153 \cdot 1 + 42$

$153 = 42 \cdot 3 + 27$

$42 = 27 \cdot 1 + 15$

$27 = 15 \cdot 1 + 12$

$15 = 12 \cdot 1 + 3$

$12 = 3 \cdot 4$

2.2) $3 = 15 - 12 \cdot 1 = 15 - (27-15) \cdot 1 = 15 \cdot 2 - 27 = (42 - 27) \cdot 2 - 27 = 42 \cdot 2 - 27 \cdot 3 = 42 \cdot 2 - (153 - 42 \cdot 3) \cdot 3 = 42 \cdot 11 - 153 \cdot 3 = (195 - 153) \cdot 11 - 153 \cdot 3 = 195 \cdot 11 - 153 \cdot 14 = 195 \cdot 11 - (543 - 195 \cdot 2) \cdot 14 = 195 \cdot 39 - 543 \cdot 14 = (123456 - 227 \cdot 543) \cdot 39 - 543 \cdot 14 = 123456 \cdot 39 - 543 \cdot 8876$

Ответ: $d=2$, $x = 39$, $y = -8876$.

Обратите внимание одно из чисел x или y отрицательно. Конечная запись представления через x и y имеет вид $d=bx+ay$, поэтому x или y имеет отрицательное значение.

Для того, чтоб убедиться в правильности проделанной работы, вычисляем последнюю разность (*123456·39–543·8876*), она должна равняться НОД(*123456, 543*), в нашем случае *3*. Расширенный алгоритм Евклида можно основываясь на формулах его числовой записи, однако существует его более удачная реализация [7, 8].

Определение: Всякое целое, кратное данных чисел $a_1, a_2, \ldots a_n$ называется их общим кратным. Наименьшее среди общих кратных есть ***наименьшее общее кратное***, записывается НОК($a_1, a_2, \ldots a_n$).

Свойства НОК

1) Совокупность общих кратных двух чисел совпадает с совокупностью кратных их наименьшего общего кратного.

2) НОК(a, b) = $\frac{a \cdot b}{НОД(a;b)}$

Из второго свойства НОК очевидно, что если a и b взаимно просты (т.е. НОД(a, b)=1), то НОК(a, b)=$a \cdot b$.

Пример

Найдем НОК(*57, 15*)

НОК(*57, 15*)=$\frac{57 \cdot 15}{3} = 285.$

Задания

Для того чтоб закрепить прочитанный материал, Вам предлагается

решить следующие задания.

1.1.1 Найти НОД с помощью АЕ

НОД(*28,35*) Ответ *7*

НОД(*112,37*) Ответ *1*

НОД(*76,336*) *4*

НОД(*45,351*) *9*

НОД(*365,45*) Ответ *5*

НОД(*603,108*) Ответ *9*

НОД(*241,37*) Ответ *1*

1.1.2 Проделать РАЕ для чисел

53, 200	*x=-83, y=22*
29,278	*x=-115, y=12*
37,178	*x=77, y=-16*
603, 108	Ответ *x = -5, y = 28*
50, 286	Ответ *x = 7, y = -40*

1.1.3 Найти НОК

15, 3	Ответ *15*
28, 35	Ответ *140*
70,136	*4760*
42,273	*546*

§II.2. ПРОСТЫЕ ЧИСЛА.

Всякое целое $a > 1$ число, имеет как минимум два делителя (1 и a), если этими числами исчерпываются все положительные делители целого числа, то оно называется ***простым***, иначе, если число имеет помимо 1 и самого себя другие положительные делители, то оно называется ***составным***.

Например, $2,3,5,7,11$ – простые числа, а $6,8,9,12$ – составные.

Число 1 имеет только один положительный делитель, а именно 1. Посему число 1 в ряде натуральных чисел стоит совершенно особо, не относится ни к простым ни к составным.

Утверждение 1

Наименьший отличный от 1 делитель целого числа a, есть число простое.

Доказательство

Пусть q – наименьший делитель a, если бы q было бы составным, то оно имело бы делитель q_1 с условием $1<q_1<q$, причем число a, делясь на q, по свойству транзитивности делимости должно делиться на q_1, но это противоречит тому, что q – наименьший делитель a. ■

Утверждение 2

Наименьший отличный от 1 делитель составного числа a не превосходит $\sqrt{a}$.

Доказательство

Пусть q наименьший $\neq 1$ делитель a, т.е. $a=q\cdot a_1$, $a_1 \geq q$ т.к. q – наименьший делитель a. Помножим $a_1 \geq q$ на q, получим $a_1\cdot q \geq q^2$, т.к. $a=q\cdot a_1$, $a \geq q^2$, откуда $q \leq \sqrt{a}$. ■

Утверждение 3 (Теорема Евклида)

Простых чисел бесконечно много.

Доказательство

Предположим, что простых чисел конечное количество и $\{p_1,p_2,\dots p_k\}$ есть все простые числа. Тогда наименьший $\neq 1$ делитель $n= p_1 \cdot p_2 \cdot \dots p_k + 1$ (по **Утверждению 1**) есть число простое и оно не совпадает не с одним из p_i, т.к. если бы совпадало, оно должно было бы делить *1*, что противоречит начальному условию. Таким образом, для любых n простых чисел можно найти $(n+1)$-е простое, что подтверждает утверждение о их бесконечности. ■

Для нахождения таблицы простых чисел, не превосходящих n, существует простой способ, называемый ***решетом Эратосфена*** [1,3,4,6]. Он заключается в следующем. Выписываем все числа от *1* до n.

$$1, 2, 3, 4, \dots n$$

Первое простое число – *2*, оно делится только на *1* и на себя, следовательно, оно простое. Вычеркиваем из ряда все числа кратные *2* кроме *2*, они будут составными, так как помимо *1* и себя имеют делитель – *2*. Следующее, не вычеркнутое число – *3*, оно простое, так как если бы оно было бы составным, то оно было бы вычеркнутым. Вычеркиваем все числа кратные *3* кроме *3*. Следующее, не вычеркнутое число – *5*. И т.д.

Составление таблицы всех простых чисел меньших n закончено сразу, как только вычеркнуты все кратные простых, меньших $\sqrt{n}$.

Данный метод позволяет строить множество простых чисел, но он неудобен для проверки простоты заданного числа. Тем не менее, идея решета и ее обобщения в настоящее время часто используются для «просеивания» множеств чисел, обладающих тем или иным условием. Более того, разрабатываются специальные микропроцессоры, на которых операции «просеива-

ния» выполняются очень эффективно [6].

Построение в настоящие время таблицы простых чисел показывают, что с ростом их величин они встречаются все реже и реже. Например, в первой сотне чисел (*n=100*) их *25*, во второй - *21*, третьей *16* и т.д. В первой *1000* их *168*, во второй тысяче – *135*, в третьей – *120* и т.д.

Для нахождения количества чисел в некотором диапазоне можно воспользоваться следующей теоремой [6].

Утверждение 4 (Теорема Чебышева)

Пусть $П(x)$ – количество простых чисел $1...x$, тогда

$$\lim_{x \to \infty} \frac{П(x)}{x} \cdot \ln(x) = 1 .$$

Из данной теоремы следует, что

- При больших x: $П(x) \approx \frac{x}{\ln x}$

- Потребуется в среднем $\ln(x)$ попыток, чтобы получить простое число от $2...x$.

Утверждение 5 (Основное свойство простых чисел)

Если p – простое и $p|ab$, то $p|a$ или $p|b$ или $p|a$ и $p|b$.

Утверждение 6 (Основная теорема арифметики)

Всякое число $a>1$ представимо единственным образом в виде произведения простых чисел (если отвлечься от порядка следования сомножителей).

Или математическим языком $\forall a > 1 \in \mathbf{Z}$ $a = p_1,p_2,\ldots p_k$, где p_i – простое $\forall i = 1...k$.

Доказательство

1) Сперва докажем существование разложения.

Пусть $p_1 \neq 1$ – наименьший делитель a, следовательно, по **Утверждению**

1, p_1 – простое, тогда $a = p_1 \cdot q_1$. Если q_1 – простое, то $a = p_1 \cdot q_1$ и есть искомое представление.

Иначе $p_2 \neq 1$ – наименьший делитель q_1, следовательно, p_2 – простое, тогда $a = p_1 \cdot p_2 \cdot q_2$. Если q_2 – простое, то $a = p_1 \cdot p_2 \cdot q_2$ и есть искомое представление.

...

Приходим, $a = p_1 p_2 \ldots p_{k-1} q_{k-1}$ и q_{k-1} – простое, тогда $a = p_1 \cdot p_2 \ldots p_k$ и есть искомое представление.

2) Докажем единственность данного представления.

Предположим, что таких представлений два

$a = p_1 p_2 \ldots p_k = t_1 \cdot t_2 \cdot \ldots \cdot t_s$, p_i и t_j - простые $\forall i = 1..k \quad j = 1...s$

$p_1 | a \Rightarrow p_1 | t_1 \cdot t_2 \cdot \ldots \cdot t_s$, по основному свойству простых $p_1 | t_j$, а поскольку p_1 и t_j - простые, получаем $t_j = p_1$.

$p_2 | t_1 \cdot t_2 \cdot \ldots t_{j-1} \cdot t_{j+1} \ldots \cdot t_s$

...

Приходим $p_k = t_j$, из чего следует, что $p_1 p_2 \ldots p_k$ и $t_1 \cdot t_2 \cdot \ldots \cdot t_s$ одна и та же последовательность. ■

Пример

Разложим на простые *1827000*.

$1827000 = 2^3 \cdot 3^2 \cdot 7 \cdot 5^3 \cdot 29$.

Отметим следующие следствия из основной теоремы арифметики.

Следствие 1

Всякое число a представимо в виде $a = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$, где $e_i \neq 0$, $p_i \neq p_j$ для $\forall i \neq j$. Данное представление называется ***каноническим разложением числа a.***

Следствие 2

Если $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ и $b = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$, то

НОД(a,b) = $p_1^{\gamma_1} p_2^{\gamma_2} \dots p_k^{\gamma_k}$ и НОК(a,b) = $p_1^{\delta_1} p_2^{\delta_2} \dots p_k^{\delta_k}$, где

$\gamma_i = \min \{\alpha_i, \beta_i\}$, а $\delta_i = \max \{\alpha_i, \beta_i\}$.

Найдем количество различных делителей $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, d – делитель a можно представить $d = p_1^{\delta_1} p_2^{\delta_2} \dots p_k^{\delta_k}$, где $0 \le \delta_i \le \alpha_i$, δ_i может принимать (α_i + *1*) значение, p^{δ_i} – независимы и всякому набору $\delta_1\ \delta_2 \dots \delta_k$ соответствует свое d. Поэтому количество общих делителей можно определить как количество всевозможных сочетаний $\delta_1\ \delta_2 \dots \delta_k$ то есть как (α_1 +*1*) (α_2 +*1*)...(α_k +*1*)

Пример

Найдем количество делителей *108*

Произведем каноническое разложение $108 = 2^2 \cdot 3^3$.

Откуда количество делителей *108*: (*2+1*)(*3+1*)=*12*, перечислим их {*1*, *2*, *3*, *4*, *6*, *9*, *12*, *18*, *27*, *36*, *54*, *108*}.

Задания

1.2.1 Разложить на простые множители

123456	Ответ $2^6 \cdot 3 \cdot 643$
8720	Ответ $2^4 \cdot 5 \cdot 109$
2300	$2^2\ 5^2\ 23$
1372	$2^2\ 7^3$
1824	$2^5\ 3\ 19$

1.2.2 Найти количество делителей

2124	*18*
1720	*16*
1360	*20*
1440	*36*
2268	*30*

§II.3. СРАВНЕНИЯ

Отношения и их свойства

Множество есть совокупность некоторых объектов.

Пусть дано два множества $\mathbf{M_1}$ и $\mathbf{M_2}$, тогда декартово произведение двух множеств есть всевозможные сочетания элементов этих множеств, математическим языком

$\mathbf{M_1}\times\mathbf{M_2}= \{(x,y),\ x\in\ \mathbf{M_1}\ \ y\in\mathbf{M_2}\}$

Пример

Даны два множества $\mathbf{M_1}=\{1,2,3\}$, $\mathbf{M_2}=\{4,5\}$.

$\mathbf{M_1}\times\mathbf{M_2}= \{(1,4),(2,4),(3,4),(1,5),(2,5),(3,5)\}$

Определение: Бинарное отношение между элементами множеств, есть подмножество их декартового произведения $\boldsymbol{\rho} = \mathbf{M_1}\times\mathbf{M_2}$.

Отношение на множестве **M** - подмножество $\mathbf{M}^2$.

Слово «бинарное» означает, что в данном отношении участвует всего два числа, пример бинарного отношения: $a\cdot b$, или a/b, или $a+b$.

Примеры

1) Дано два множества $\mathbf{M_1}=\{1,2,3\}$ и $\mathbf{M_2}=\{4,5\}$, $a\subset\mathbf{M_1}$, $b\subset\mathbf{M_2}$, найти множество их бинарного отношения $\boldsymbol{\rho}$, удовлетворяющего условию

$a\boldsymbol{\rho}b \leftrightarrow a|b$ (читается: a вступает в отношения **ρ** с b если a делит b нацело).

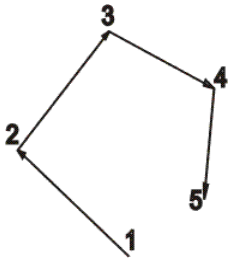
Множество, удовлетворяющее данному соотношению **ρ**={(*1*,*4*),(*1*,*5*),(*2*,*4*)}

Здесь перечислены все элементы множества $\mathbf{M_1}$ которые делятся нацело на $\mathbf{M_2}$.

2) Приведем пример бинарного отношения на одном множестве. Дано множество **M**={*1*,*2*,*3*,*4*,*5*}, a, $b \subset \mathbf{M}$. Найдем множество их бинарного отношения $a\boldsymbol{\rho}b \leftrightarrow a|b$. **ρ**={(*1*,*1*),(*1*,*2*),(*1*,*3*),(*1*,*4*),(*1*,*5*),(*2*,*2*),(*2*,*4*),(*3*,*3*),(*4*,*4*),(*5*,*5*)}.

3) Дано множество **M**={*1*,*2*,*3*} и a, $b \subset \mathbf{M}$. Найдем множество их бинарного отношения $a\boldsymbol{\rho}b \leftrightarrow a<b$. **ρ**={(*1*,*2*),(*1*,*3*),(*2*,*3*)}.

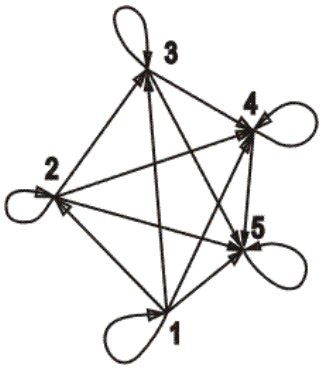
4) Дано множество **M**={*1*,*2*,*3*,*4*,*5*}, a, $b \subset \mathbf{M}$. Найдем множество их бинарного отношения $a\boldsymbol{\rho}b \leftrightarrow a=b+1$. **ρ**={(*1*,*2*),(*2*,*3*),(*3*,*4*),(*4*,*5*)}. Отношения можно задать в виде графа, для последнего примера можно построить следующий граф.



5) Дано множество **M**={*1*,*2*,*3*,*4*,*5*} и a, $b \subset \mathbf{M}$. Найдем множество их бинарного $a\boldsymbol{\rho}b \leftrightarrow a \leq b$ отношения и построим граф. Множество:

ρ={(*1*,*1*),(*1*,*2*),(*1*,*3*),(*1*,*4*),(*1*,*5*),(*2*,*2*),(*2*,*3*),(*2*,*4*),(*2*,*5*),(*3*,*3*),(*3*,*4*),(*3*,*5*),(*4*,*4*

),(*4*,*5*),(*5*,*5*)}, граф:



1 удовлетворяет данному условию для всего множества, *2* для всех чисел кроме *1*(т.к. ¬*2*<*1*), *3* для всех кроме *1* и *2*, и т.д. Еще один важный момент, *1*ρ*2*, но ¬*2*ρ*1*, поэтому используются стрелочки, указывающие какой элемент с каким вступает в отношение, если бы *1*ρ*2* и *2*ρ*1* тогда можно было бы без них обойтись, либо рисовать их с обеих сторон ребер графа.

Свойства отношений

1) ***Рефлективность***. Говорят, что отношение обладает свойством рефлективности, если для любого *a* верно *a*ρ*a*. Пример отношений, обладающих свойством рефлективности *a*ρ*b* ↔ *a*=*b* и *a*ρ*b* ↔ *a*|*b*.

2) ***Симметричность***. Говорят, что отношение обладает свойством симметричности, если для любых *a* и *b* верно, что если *a*ρ*b* ⇒ *b*ρ*a*. Например, рефлективные следующие отношения: *a*ρ*b* ↔ *a*=*b* и *a*ρ*b* ↔ *a* - *b*<*10*.

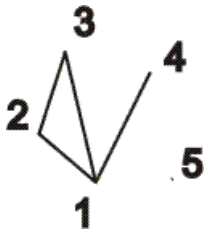
3) ***Антисимметричность***. Говорят, что отношение обладает свойством антисимметричности, если для любых *a* и *b* выполняется *a*ρ*b* ⇒ *b*ρ*a*.

4) ***Транзитивность***. Говорят, что отношение обладает свойством транзитивности, если для любых *a* и *b* выполняется *a*ρ*b* и *b*ρ*c* => *a*ρ*c*. Целочисленное деление (*a*ρ*b* ↔ *a*|*b*) обладает свойством транзитивности.

Примеры

1) Дано множество **M**={*1,2,3,4,5,6*} и *a*, *b*⊂**M**. Найдем множество их бинарного отношения

*a***ρ***b* ↔ *a*+*b*<*6*, построим граф и определим, какими свойствами оно обладает. Множество бинарного отношения **ρ**={(*1*,*2*),(*1*,*3*),(*1*,*4*),(*2*,*3*)}. Граф



Свойства:

а) Отношение не рефлективно, поскольку не для любого *a* верно *a*+*a*<*6*.

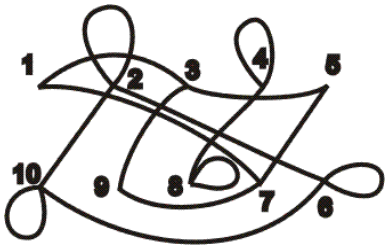
б) Симметрично, так как *1*+*3*=*3*+*1*<*6*.

в) Не антисимметрично, поскольку обладает свойством симметричности.

г) Не транзитивно, так как *4*+*1*<*6* и *1*+*2*<*6*, однако ¬*4*+*2*<*6*.

2) Дано множество **M**={*1,2,3,4,5,6,7,8,9,10*}, *a*, *b*⊂**M**. Найдем множество их бинарного отношения *a***ρ***b* ↔ *4*|(*a*+*b*) , построим граф и определим, какими свойствами оно обладает. Множество бинарного отношения

ρ={(*1*,*3*),(*1*,*7*),(*2*,*2*),(*2*,*6*),(*2*,*10*),(*3*,*5*),(*3*,*9*),(*4*,*4*),(*4*,*8*),(*5*,*7*),(*6*,*6*),(*6*,*10*),(*7*,*9*),(*8*,*8*), (*10*,*10*)}.



Свойства:

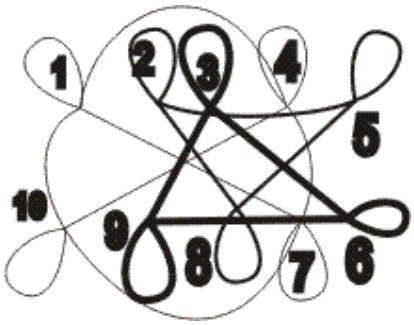
а) Не рефлективно, поскольку ¬ *4*|(*9*+*9*).

б) Симметрично, поскольку если *4*|(*a*+*b*), верно и *4*|(*b*+*a*).

в) Не антисимметрично.

г) Не транзитивно, *4*|(*5*+*7*) и *4*|(*7*+*9*), ¬ *4*|(*5*+*9*).

3) Дано множество **M**={*1,2,3,4,5,6,7,8,9,10*}, *a*, *b*⊂**M**. Найдем множество их бинарного отношения *a***ρ***b* ↔ *3*|(*a*-*b*), построим граф и определим, какими свойствами оно обладает. Множество бинарного отношения **ρ**={(*1*,*1*), (*1*,*4*), (*1*,*7*), (*1*,*10*), (*2*,*2*), (*2*,*5*), (*2*,*8*), (*3*,*3*), (*3*,*6*), (*3*,*9*), (*4*,*4*), (*4*,*7*), (*4*,*10*), (*5*,*5*), (*5*,*8*),(*6*,*6*), (*6*,*9*), (*7*,*7*), (*7*,*10*), (*8*,*8*), (*9*,*9*), (*10*,*10*)}.



Свойства:

а) Рефлексивно, поскольку *3*|(*a*-*a*).

б) Симметрично, поскольку если *3*|(*a*-*b*), верно и *3*|(*b*-*a*), т.к (*b*-*a*) и (*a*-*b*) отличаются только знаком.

в) Не антисимметрично.

г) Транзитивно.

Данное отношение является уникальным в своем роде. Обратите внимание все множество **M** разбилось на три части (для каждой из частей используется своя толщина линии). Данное отношение называется отношением эквивалентности. Отношение со свойствами рефлективность, симметричность и транзитивность называется ***отношением эквивалентности*** [2,8]. Замечательная особенность отношения эквивалентности в том, что по нему множество, на котором оно определено разбивается на непересекающиеся классы (классы эквивалентности) и отношение выполняется если числа, вступающие в отношение, принадлежат одному классу.

В нашем случае отношение разбилось на классы $\mathbf{M_1}=\{1,4,7,10\}$, $\mathbf{M_2}=\{2,5,8\}$ и $\mathbf{M_3}=\{3,6,9\}$ и отношение выполняется т.е $3|(a-b)$ если a и b принадлежат одному классу.

Перейдем, к основной цели данного параграфа - к сравнениям [1,3].

Определение: Пусть $a, b \in \mathbf{Z}$, $m \in \mathbf{N}$. Говорят, что число a сравнимо с b по модулю m, если a и b при делении на m дают одинаковые остатки. Запись этого факта выглядит так: $a \equiv b(\mathrm{mod}\ m)$, верно и $a \equiv b \mod m$. Однако первый вид записи нам кажется более приемлемым, что запись $(\mathrm{mod}\ m)$ имеет отношение к обеим частям. Зачастую вместо символа “≡” можно встретить “=”.

Математическим языком данное определение можно записать как

$$a \equiv b(\mathrm{mod}\ m) \Leftrightarrow a \bmod m = b \bmod m \qquad (1)$$

Иначе сей факт можно записать как

$a \equiv b \pmod{m} \Leftrightarrow \exists t$ такое, что $a = b + m \cdot t$ (2)

$a \equiv b \pmod{m} \Leftrightarrow m|(a-b)$ (3)

Данные факты (2) и (3) являются из разряда очевидных. В дальнейшем к данным записям мы будем обращаться как к (1), (2) и (3) записи сравнения.

Примеры

$5 \equiv 13 \pmod{7}$

$7 \equiv -3 \pmod{10}$ по (2) записи сравнения $7 = -3 + 10 \cdot 1$

$8 \equiv -2 \pmod{5}$, по (2) $8 \equiv -2 + 5 \cdot 2$

Свойства сравнений

Отметим важную деталь сравнений чисел по модулю. Сравнение чисел по некоторому модулю есть бинарное отношение, которое обладает следующими свойствами

1) Рефлективность, так как $a \equiv a \bmod m$.

2) Симметричность, поскольку если $a \equiv b \bmod m$, то верно $b \equiv a \bmod m$.

3) Транзитивность: $a \equiv b \bmod m$ и $b \equiv c \bmod m \Rightarrow a \equiv c \bmod m$.

Отсюда получаем, что сравнение чисел по модулю есть отношение эквивалентности [1]. То есть всё множество **Z** по сравнению разбивается на классы эквивалентности.

Пример

1) Сравнение по модулю *2* определено на множестве **Z,** покажем на

какие классы разбивается множество. Имеется только два вида остатков от деления на *2* - *0* и *1*, следовательно, классов будет два: класс чисел остаток от деления на *2* которых равен *0* и класс дающих остаток *1*.

1-й класс [*0*] = {*0*; ±*2*; ±*4*; … }, все числа при делении на *2* дающие остаток *0*.

2-й класс [*1*] = {±*1*; ±*3*; ±*5*; …}, все числа при делении на *2* дающие остаток *1*.

2) Модуль равен *4*, продемонстрируем классы разбиения множества **Z**

Возможно *4* остатка от деления на *4* (*0*,*1*,*2*,*3*), аналогично количество классов

[*0*] = {…*-16*,*-12*,*-8*,*-4*,*0*,*4*,*8*,*12*,*16*,…}, числа при делении на *4* дающие остаток 0.

[*1*] = {…,*-15*,*-11*,*-7*,*-3*,*1*,*5*,*9*,*13*,…}, числа при делении на *4* дающие остаток *1*.

[*2*] = {…,*-14*,*-10*,*-6*,*-2*,*2*,*6*,*10*,*14*,…}, числа при делении на *4* дающие остаток *2*.

[*3*] = {…,*-13*,*-9*,*-5*,*-1*, *3*, *7*, *11*, *15*,…}, числа при делении на *4* дающие остаток *3*.

Обозначение вида [*1*] читается класс вычетов по некоторому модулю, содержащий число *1*. Для второго примера верно [*1*] = [*9*] = [*-7*], поскольку это один и тот же класс, верно и [*-2*] = [*6*] = [*10*] = [*-14*]. Любое число из класса вычетов будем называть вычетом по модулю *m*.

4) Сравнения по одинаковому модулю можно почленно складывать.

Доказательство

Пусть $a_1 \equiv b_1 (\text{mod } m)$, $a_2 \equiv b_2 (\text{mod } m)$. Это означает, что $a_1 = b_1 + mt_1$, $a_2 = b_2 + mt_2$. После сложения последних двух равенств получим $a_1 + a_2 = b_1 + b_2 + m(t_1 + t_2)$, что означает $a_1 + a_2 \equiv b_1 + b_2 (\text{mod } m)$.■

5) Слагаемое, стоящее в какой-либо части сравнения, можно переносить в другую часть, изменив его знак на обратный.

Доказательство

$a_1 + a_2 + \ldots + r \equiv b_1 + b_2 + \ldots (\text{mod } m)$.

Из 4-го свойства можем прибавить $-r \equiv -r (\text{mod } m)$, получим

$a_1 + a_2 + \ldots \equiv b_1 + b_2 + \ldots - r (\text{mod } m)$ ■

6) К любой части сравнения можно прибавить любое число, кратное модулю.

Доказательство

Пусть $a \equiv b (\text{mod } m)$ и пусть d кратно m, т.е. $d = m \cdot c$. Отсюда $a = b + mt$. После сложения последних двух равенств получим $a + d = b + m(t + c)$, что означает $a + d \equiv b (\text{mod } m)$. ■

7) Сравнения по одинаковому модулю можно почленно перемножать.

Доказательство

Пусть $a_1 \equiv b_1 (\text{mod } m)$, $a_2 \equiv b_2 (\text{mod } m)$. Это означает, что $a_1 = b_1 + mt_1$, $a_2 = b_2 + mt_2$.После умножения последних двух равенств получим $a_1 a_2 = b_1 b_2 + b_1 \cdot m \cdot t_2 + m \cdot t_1 \cdot b_2 + m^2 \cdot t_1 \cdot t_2 = b_1 \cdot b_2 + m(b_1 \cdot t_2 + t_1 \cdot b_2 + m \cdot t_1 \cdot t_2)$, что, по (2) записи сравнения означает $a_1 + a_2 \equiv b_1 + b_2 (\text{mod } m)$.■

И как следствие **7**:

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

9) Обе части сравнения и его модуль можно умножить на одно и то же целое число или разделить на их общий делитель.

Доказательство

$a \equiv b \pmod{m} \Leftrightarrow a=b+mt \Leftrightarrow ak=bk+mkt \Leftrightarrow ak \equiv bk \pmod{mk}$.■

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

Доказательство

Если $a \equiv b \pmod{m_1}$ и $a \equiv b \pmod{m_2}$, то $a-b$ (по (3) записи сравнения) делится на m_1 и на m_2, значит $a-b$ делится на наименьшее общее кратное m_1 и m_2.■

11) Если сравнение имеет место по модулю m, то оно имеет место и по модулю d, равному любому делителю числа m.

Доказательство очевидно следует из транзитивности делимости: если $a \equiv b \pmod{m}$, то по (3) записи сравнения $a-b$ делится на m, значит $a-b$ делится на d , где $d|m$. ■

Определение: Совокупность из m (штук) попарно несравнимых по модулю m чисел есть ***полная система вычетов*** [1,3].

Напомним, любое число из класса вычетов $[a]$ называется вычетом сравнимым с a по модулю m. Тогда полная система вычетов есть множество вычетов, взятых по одному из каждого класса вычетов $[1],[2],...[m-1]$. Непосредственно сами остатки при делении на m $(1, 2,\ldots m-1)$ называются наименьшими неотрицательными вычетами и, конечно, образуют полную систему вычетов по модулю m. Вычет r называется абсолютно наименьшим, если $|r|$ наименьший среди модулей вычетов данного класса.

Пример

Приведем полную систему абсолютно наименьших, наименьших неотрицательных и случайную систему вычетов по модулю *7*.

Перечислим все возможные классы вычетов по модулю *7*

[*0*],[*1*],[*2*],[*3*],[*4*],[*5*],[*6*] - все классы вычетов по модулю *7*, беря из каждого класса по одному числу получим полную систему вычетов.

{*0,1,2,3,4,5,6*} - полная система наименьших неотрицательных вычетов.

{*-3,-2,-1,0, 1, 2, 3*} - полная система абсолютно наименьших вычетов.

{*35,50,-5,3,67,-9,-8*}- эта совокупность тоже является полной системой вычетов.

Для обозначения используется $\mathbf{Z}_7$.

$\mathbf{Z}_7$={*0,1,2,3,4,5,6*} или $\mathbf{Z}_7$={*35,50,-5,3,67,-9,-8*}

Найти полную систему вычетов по модулю *m* очень просто, для этого нам нужно найти всевозможные остатки от деления на *m*, то есть: *0, 1, 2, … m-1*.

Лемма 3.1

Если НОД(*a*, *m*)=*1* и *x* пробегает полную систему вычетов по модулю *m*, то значения линейной формы *ax*+*b* , где *b* - любое целое число, тоже пробегают полную систему вычетов по модулю *m*.

Доказательство

Чисел *ax*+*b* ровно *m* штук, столько же сколько *x*. Покажем, что они между собой не сравнимы по модулю *m*. Пусть для некоторых различных x_1 и x_2 из полной системы вычетов оказалось, что $ax_1 + b \equiv ax_2 + b \pmod m$. Тогда, по 4-му свойству сравнений можем сложить с

$-b \equiv -b \pmod m$,

получаем:

$a \cdot x_1 \equiv a \cdot x_2 \pmod{m}$.

По 9-му свойству сравнения можем помножить на $a^{-1} \equiv a^{-1} \pmod{m}$, получим

$x_1 \equiv x_2 \pmod{m}$

– что противоречит тому, что x_1 и x_2 различны т.к. взяты из полной системы вычетов. ■

Определение. ***Приведенной системой вычетов*** по модулю m называется совокупность всех вычетов из полной системы >0 и взаимно простых с модулем m. Обозначается приведенная система вычетов $\mathbf{U_m}$.

Пример

1) Найдем приведенную систему вычетов по модулю 7.

Полная система вычетов имеет вид $\mathbf{Z}_7=\{0,1,2,3,4,5,6\}$, чтобы найти приведенную систему необходимо проверить на взаимную простоту с $m=7$ каждый из элементов полной системы вычетов. Поскольку 7 – число простое (стало быть, оно имеет только 2 делителя – 1 и 7), то в нашем случае числа $1,2,3,4,5,6$ не имеют общих делителей с 7 кроме 1, т.е. $1,2,3,4,5,6$ это и есть все не нулевые вычеты взаимно простые с m.

$\mathbf{U}_7=\{1,2,3,4,5,6\}$

2) Найдем приведенную систему вычетов по модулю 9.

Полная система вычетов по модулю 9 $\mathbf{Z}_9=\{0,1,2,3,4,5,6,7,8\}$, найдем НОД($i$,9) для каждого из $1,2,3,4,5,6,7,8$

НОД(1, 9)=1, то есть 1 и 9 - взаимнопросты

НОД(2, 9)=1, то есть 2 и 9 - взаимнопросты

НОД(3, 9)=3, то есть 3 и 9 – не взаимнопросты

НОД(4, 9)=1, то есть 4 и 9 - взаимнопросты

НОД(*5*, *9*)=*1*, то есть *5* и *9* - взаимнопросты

НОД(*6*, *9*)=*3*, то есть *6* и *9* – не взаимнопросты

НОД(*7*, *9*)=*1*, то есть *7* и *9* - взаимнопросты

НОД(*8*, *9*)=*1*, то есть *8* и *9* - взаимнопросты

$\mathbf{U_9} = \{0,1,2,4,5,7,8\}$.

Определение: Пусть на некотором множестве **M** определена бинарная операция ○, элемент *e* называется нейтральным относительно данной операции, если для $\forall a \in \mathbf{M}$ выполняется $a \circ e = e \circ a = a$. Элемент *b* называется обратным к *a* если $a \circ b = b \circ a = e$.

Пример

На множестве **Z**, можно определить операции сложения и умножения. Для умножения нейтральным будет 1, т.к. $a \cdot 1 = 1 \cdot a = a$, для сложения нейтральным будет *0*, т.к. $a+0=0+a=a$.

Обратный элемент определяется для каждого элемента индивидуально, лишь в некоторых случаях можно привести универсальную формулу для всех. Для сложения обратным к *a* будет $-a$, т.к. $a+(-a)=(-a)+a=0$, для умножения можно определить обратный только для *-1* и *1*, обратным будет *-1* и *1* соответственно.

Для нас важным будет понятие обратимости по модулю, итак

Определение: Элемент *b* называется обратным к *a* по модулю *m* если $a \cdot b \equiv 1 \bmod m$. Элемент *a* называется обратимым если для него существует обратный.

Пример

$2^{-1} \bmod 5 \equiv 3$, т.к. $2 \cdot 3 \equiv 6 \equiv 1 \bmod 5$

$7^{-1} \bmod 11 \equiv 8$, т.к. $7 \cdot 8 \equiv 56 \equiv 1 \bmod 11$

$4^{-1} \bmod 7 \equiv 2$, т.к. $4 \cdot 2 \equiv 1 \bmod 7$

$11^{-1} \bmod 7$, то же самое, что $4^{-1} \bmod 7$, поскольку по модулю 4 и 11 принадлежат одному классу вычетов по модулю7. Из предыдущего примера $4^{-1} \bmod 7 \equiv 2$, значит $11^{-1} \bmod 7 \equiv 2$. Проверим $11 \cdot 2 \equiv 22 \equiv 1 \bmod 7$.

Обратный к данному элемент не всегда существует, например обратный к 2 по модулю 8 не определен. Следующей теоремой определим, в каких случаях существует обратный к заданному элементу по некоторому модулю [1,3].

Теорема обратимости

Элемент a обратим по модулю m если и только если НОД(a, m)=1.

Доказательство

1) Необходимость. По определению обратимости имеем $a \cdot b \equiv 1 \bmod m$, по (2) форме записи сравнения имеем $a \cdot b = 1 + m \cdot t$. Пусть d=НОД(a, m), тогда $d|a \Rightarrow d|ab$, $d|m \Rightarrow d|mt$. Из (2) записи сравнения получаем $d|1$.

2) Докажем достаточность.

НОД(a,m)=1следовательно по алгоритму Евклида имеет место следующее представление $a \cdot x + m \cdot t = 1$, данная запись есть (2) форма записи сравнения, следовательно $a \cdot x \equiv 1 \bmod m$. ■

Теперь сформируем еще одно определение приведенной системой вычетов [1]. Поскольку из взаимно простоты следует обратимость, а из обратимости взаимно простота по модулю m имеет место следующее определение.

Определение: Совокупность из всех обратимых попарно несравнимых по модулю m чисел есть приведенная система вычетов.

Обычно приводят приведенную систему минимальных положительных вычетов по модулю. Для ее составления обычно берут полную систему вычетов и оставить только те, которые взаимно просты с модулем.

Пример

Полная система вычетов по модулю *7*: $\mathbf{Z_7}=\{0,1,2,3,4,5,6\}$. Из этого множества оставим только те, которые взаимно просты с *7*, т.е. $\mathbf{U_7}=\{1,2,3,4,5,6\}$.

$\mathbf{U_7}$	x	1	2	3	4	5	6
	x^{-}	1	4	5	2	3	6

Полная система вычетов по модулю *18*: $\mathbf{Z_{18}}=\{0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17\}$. Из этого множества оставим только те, которые взаимно просты с *18*, т.е. $\mathbf{U_{18}}=\{1,5,7,11,13,17\}$.

В приведенной системе вычетов по определению для каждого существует обратный. Для приведенных примеров составим таблицы

$\mathbf{U}_{18}$	x	1	5	7	1	1	1
	x^{-}	1	1	1	5	7	1

Приведенная система вычетов по простому модулю, *p* - простое $\mathbf{U_p}=\mathbf{Z_p}-\{0\}$.

Заметим, $(m-1)^{-1} \equiv (m-1) \bmod m$. Читателю рекомендуется доказать.

Нахождение обратного к заданному по модулю m

По алгоритму Евклида знаем, что если НОД(*a*, *b*)=*1*, то можем придти к следующей записи $a \cdot x + m \cdot t = 1$, эта запись подобна второй записи сравнения.

Можем записать $a \cdot x \equiv 1 \bmod m$, тогда обратным к a будет x.

Пример

Найдем $13^{-1} \bmod 30$

Сперва проверим существование обратного, т.е. проверим условие НОД(*13,30*)=*1*.

$30=13 \cdot 2+4$

$13=4 \cdot 3+1$

$4=1 \cdot 4$

$1=13-4 \cdot 3=13-(30-13 \cdot 2)3=13 \cdot 7+30 \cdot 3$

Обратный к *13* есть умножаемое на него, то есть *7*.

Проверим $13 \cdot 7 \bmod 30 \equiv 91 \equiv 1 \bmod 30$.

Ответ: $13^{-1} \pmod{30} = 7$

Задания

1.3.1 Какими свойствами обладают отношения

$a \rho b \leftrightarrow a+b|2$, *определенное на* **Z**

$a \rho b \leftrightarrow (a-2)|b$ *определенное на* **Z**

$a \rho b \leftrightarrow (a+b)>(ab)$ *определенное на* **Z**

1.3.2 Найти

$74^{-1} \bmod 163$ Ответ -11

$50^{-1} \bmod 286$ *решений нет*

$52^{-1} \bmod 287$ *138*

$45^{-1} \bmod 228$ *решений нет*

$86^{-1} \bmod 113$ *46*

$39^{-1} \bmod 149$ *-42*

$68^{-1} \bmod 399$ *-88*

1.3.3 Найти полную и приведенную системы наименьших вычетов по следующим модулям

14 *Полная:* {*0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13*}, *приведенная:* {*1, 3, 5, 9, 11, 13*}

15 *Полная:* {*0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14*}, *приведенная*: {*1, 2, 4, 7, 8, 11, 13, 14*}

16 *Полная:* {*0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15*}, *приведенная:* {*1, 3, 5, 7, 9, 11, 13, 15*}

17 *Полная:* {*0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16*}, *приведенная*: {*1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16*}

§II.4. ФУНКЦИЯ ЭЙЛЕРА

Функция Эйлера, пожалуй, самая знаменитая функция из всех функций, рассматриваемых в теории чисел.

Леонард Эйлер (1707-1783) - великий математик [11,12], механик и физик. Родившись в Базеле (Швейцария) в семье пастора, Леонард получил первоначальное образование у своего отца - ученика знаменитого математика Якова Бернулли. По окончании средней школы по настоянию отца он поступил на теологический факультет Базельского университета.

Однако Эйлер интересовался не теологией, а математикой. Он стал слушать лекции известного профессора математики Иоганна Бернулли, младшего брата Якова Бернулли.

В 1727 г. Эйлер приехал в Петербург, получив место адъюнкт-профессора в недавно основанной Академии наук и художеств. В 1733 г. он женился на Е. Гзелль дочери академического живописца.

Тревожное положение в политической жизни в нашей стране после смерти царевны Анны Иоанновны заставило Эйлера в 1741 г. переехать в Берлин, где он занял должность директора класса математики и члена правления Берлинской Академии наук. Однако учёный сохранял тесные связи с Петербургской Академией наук и поддерживал переписку с М.В. Ломоносовым и другими русскими учёными.

В 1766 Эйлер со всей своей семьёй вернулся в Петербург, где и работал до последнего дня жизни. В России Эйлер прожил 31 год, став главой русской математической школы. Многие дети и внуки Эйлера по сей день проживают в России.

Как и любой гений Эйлер был необыкновенно трудолюбивым, настолько, что в результате напряженной работы ещё в 1735 г. лишился правого глаза, а в 1766 г. потерял и второй глаз, катаракта, которая сейчас легко лечится, лишила его зрения. Часть своих трудов слепой учёный диктовал писцу. О работоспособности Эйлера на склоне лет говорит такой феноменальный факт: за 1777 г. он с секретарем подготовил около 100 статей, т.е. почти по две статьи в неделю. Всего им было написано более 850 статей и трудов. Эйлер умер в 1783 в возрасте 76 лет от кровоизлияния в мозг, и был похоронен в Петербурге на Смоленском кладбище.

Определение: Функция Эйлера определена только для положительных целых чисел. Функция Эйлера $\varphi(a)$ есть количество чисел из ряда *0,1,2,..., a-1*, взаимно простых с *a*.

Пример

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

$\varphi(2)=1$ $\varphi(4)=2$ $\varphi(6)=2$

Функция Эйлера есть мощность приведенной системы вычетов $|\mathbf{U_a}| = \varphi(a)$, мощность приведенной системы вычетов есть количество чисел в ней, что соответствует определению функции Эйлера [].

Для маленьких чисел найти функцию Эйлера несложно, но для больших пересчитывать все числа взаимно простые с *a*, не самая приятная перспектива. Поэтому найдем простой способ вычисления функции Эйлера, но сперва дадим несколько свойств.

Свойства функции Эйлера

1) Функция Эйлера мультипликативная [1], то есть для любых a и b таких что НОД(a,b)=*1* $\varphi(a\cdot b)=\varphi(a)\cdot\varphi(b)$.

Для доказательства данного факта нам понадобится сформулировать и доказать лемму.

Лемма 4.1

НОД($a\cdot b$, n) = *1* $\Leftrightarrow$ НОД(a, n) = НОД(b, n) = *1*

Доказательство

1) Необходимость: Известно НОД(ab, n) = *1*, пусть d = НОД(a, n)

$$\left.\begin{array}{l} d|a \\ d|ab \\ d|n \end{array}\right\} \Rightarrow \quad d|\text{НОД}(ab,n) \quad =1 \quad \Rightarrow \quad d|1 \quad \Rightarrow \quad d=\text{НОД}(a,n)=1.$$

Аналогично доказательство НОД (b, n) =*1*.

2) Достаточность: Известно НОД(a,n) = НОД(b,n) = *1*, пусть d = НОД (ab; n). Пусть p - простое и пусть

$$p|d \Rightarrow p|a\cdot b \Rightarrow \text{(по осн. св. простых)}\} \Rightarrow p|\text{HOD}(a,n) \text{ или } p|\text{НОД}(b,n)\Rightarrow$$

$p|a$ или $p|b$

$p|n$

$\Rightarrow p|1 \Rightarrow d = 1$.■

Докажем свойство мультипликативности функции Эйлера.

Доказательство

НОД(a, b) = *1*

$\varphi(a\cdot b)$-количество чисел в ряду *1*,*2*,...$a\cdot b$ *-1* взаимно простых с $a\cdot b$, а по **Лемме 4.1** это количество чисел одновременно взаимно простых с a и взаимно простых с b.

Построим таблицу следующего вида

1	*2*	…	*B*
b+1	*b+2*	…	*2·b*
…			
(a-1)·b +1	*(a-1)·b +2*	…	*a·b*
r=1	*r=2*	…	*r=0*

В таблице перечислены все числа в диапазоне *1…a·b*.

В каждой строке числа вида $b \cdot x + r \equiv r \pmod{b}$, где $r \in [1 \ldots b]$, то есть каждая строка есть полная система вычетов и в ней $\varphi(b)$ чисел взаимно простых с *b*. Все числа в столбцах имеют остаток от деления на *b* одно и то же число, таким образом $\varphi(b)$столбцов взаимно простых с *b*.

В каждом столбце числа вида *b·x+r*, по условию НОД(*a*, *b*)=*1*, по **Лемме 3.1** каждый столбец есть полная система вычетов по модулю *a*.

$\varphi(b)$ столбцов взаимно простых с *b* и в каждом столбце $\varphi(a)$ чисел взаимно простых с *a*, из чего получаем $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$. ■

Продолжим свойства функции Эйлера.

2) Если *p* – простое, то $\varphi(p) = p-1$.

Доказательство

$\varphi(p)$ – количество чисел в ряду *1…p-1* взаимно простых с *p*, но в данном ряду все числа взаимно просты с *p*.

3) Для простого *p* - $\varphi(p^k) = p^k - p^{k-1} = p^k \left(1 - \frac{1}{p}\right)$

Доказательство

По определению функции Эйлера $\varphi(p^k)$ – это количество чисел в ряду *1*, *2*, … p^k взаимно простых с p^k. Поскольку *p* – простое, то не взаимно просты-

ми с p^k будут все числа вида $pt \le p^k$. Преобразуем последнее неравенство в следующий вид $t \le p^{k-1}$, из последнего соотношения видно, что не взаимно простых в данном ряду – t чисел, где $t \in \{1,2,\dots p^{k-1}\}$. Получили, в ряду p^k чисел, из них p^{k-1} не взаимно простых с p^k, то есть $\varphi(p^k) = p^k - p^{k-1}$

Обобщим вышеизложенные свойства. Для вычисления функции Эйлера для некоторого числа сперва произведем его каноническое разложение в вид $a = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$, где $e_i \neq 0$, $p_i \neq p_j$ для $\forall i \neq j$, затем поскольку $p_i \neq p_j$ то есть они взаимно просты (т.е. НОД(p_i,p_j)=1), поэтому

$$\varphi(a) = \varphi(p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}) = \varphi(p_1^{e_1})\varphi(p_2^{e_2})\dots\varphi(p_k^{e_k}) =$$
$$= (p_1^{e_1} - p_1^{e_1-1})(p_2^{e_2} - p_2^{e_2-1})\dots(p_k^{e_k} - p_k^{e_k-1}) = a(1-\frac{1}{p_1})(1-\frac{1}{p_2})\dots(1-\frac{1}{p_k})$$

Теорема Эйлера

Пусть НОД(a, n)=1, тогда $a^{\varphi(n)} \equiv 1 (\mathrm{mod}\ n)$

Доказательство

Рассмотрим $\{x_1, x_2, \dots x_n\}$ приведенную систему вычетов, НОД($a \cdot x_i$, n) = 1, для любого $i = 1 \dots \varphi(n)$ т.к. НОД(a, n) = 1 и $a \cdot x_i$ взаимно простые с n по **Лемме 4.1**.

$a \cdot x_i \neq a \cdot x_j \pmod n$ для любого $i \neq j$, тогда $\{a \cdot x_1, a \cdot x_2, \dots a \cdot x_{\varphi(n)}\}$ также приведенная система вычетов. Пусть z_i соответствующие $a \cdot x_i$ наименьшие неотрицательные вычеты, тогда

$a \cdot x_1 \equiv z_1 \bmod n$

$a \cdot x_2 \equiv z_2 \bmod n$

…

$a \cdot x_{\varphi(n)} \equiv z_{\varphi(n)} \bmod n$

Перемножив почленно данные сравнения получим

$a^{\varphi(n)} \cdot x_1 \cdot x_2 \ldots x_{\varphi(n)} \equiv z_1 \cdot z_2 \cdot \ldots \cdot z_{\varphi(n)} \bmod n$

Причем $x_1 \cdot x_2 \ldots x_{\varphi(n)} \equiv z_1 \cdot z_2 \cdot \ldots \cdot z_{\varphi(n)} \bmod n$, поскольку отличаются только порядком сомножителей, поэтому можем записать

$a^{\varphi(n)} \cdot x_1 \cdot x_2 \ldots x_{\varphi(n)} \equiv x_1 \cdot x_2 \ldots x_{\varphi(n)} \bmod n$

Поскольку $x_1 \cdot x_2 \ldots x_{\varphi(n)}$ произведение элементов из приведенной системы вычетов то НОД $(x_1 \cdot x_2 \ldots x_{\varphi(n)}, n) = 1$ и можем осуществить следующий переход

$a^{\varphi(n)} \equiv 1 \bmod n$ ■

Пьер Ферма (1601 - 1665) родился и умер в маленьком городке Бомоне[13] на левом берегу Гаронны вблизи Монтабане-на-Тарне (во Франции более 30 Бомонов), где 34 года исправно служил чиновником кассационной палаты Тулузского парламента. Ферма почти не выезжал из Тулузы, где осел после женитьбы на кузине своей матери Луизе де Лон, дочери советника того-самого парламента. Благодаря тестю он дослужился до звания советника и приобрел вожделенную приставку "де".

Интерес к математике обозначился у Ферма как-то неожиданно и в достаточно зрелом возрасте. В 1629 г. в его руки попадает латинский перевод работы Паппа, содержащий краткую сводку результатов Аполлония о свойствах конических сечений. Ферма, полиглот, знаток права и античной филологии, вдруг задается целью полностью восстановить ход рассуждений знаменитого ученого. С таким же успехом современный адвокат может попытаться самостоятельно воспроизвести все доказательства в монографии по алгебраической топологии. Однако, немыслимое предприятие увенчивается успехом.

Чиновникам провинциальных судов предписывалось вести замкнутую жизнь, избегая любых проявлений публичности. Вероятно Ферма, считая себя солидным человеком, стеснялся своей страсти к досужим формаль-

ным играм. На склоне лет наш герой пишет: "Так как, говоря откровенно, я считаю геометрию самым высоким упражнением для ума, но одновременно столь бесполезным, что я делаю мало различия между человеком, который занимается только геометрией, и искусным ремесленником. Я называю геометрию самой прекрасной профессией в мире, но все же только профессией , и я часто говорю, что она хороша для пробы сил, но не для того, чтобы вкладывать в нее все силы..." . Он изменил себе лишь перед смертью, опубликовав в Тулузе далеко не самые блестящие из своих находок в небольшом трактате "О сравнении кривых линий прямыми". Ферма неожиданно умирает в возрасте 64 лет во время поездки по делам службы.

Его прижизненная известность основана на обильной переписке, в которой он донимал друзей и недругов необычными задачами. Его посмертная слава разрослась благодаря скромным пометкам на полях "Арифметики" Диофанта. Обычно человечеству необходимо несколько десятков лет, чтобы разобраться с наследием очередного неуемного гения. На окончательное осмысление загадок Ферма понадобилось без малого четыре века

Малая теорема Ферма

Пусть p – простое число и p не делит a, тогда: $a^{p-1} \equiv 1 \pmod{p}$

Доказательство

Положим в условии теоремы Эйлера $n = p$, где p -простое, тогда $\varphi(n)=p-1$. Получаем

$a^{p-1} \equiv 1 \pmod{p}$.

Следствие

Для любого $a \in \mathbf{Z}$, $a^p \equiv a \pmod{p}$.

Доказательство

Умножим обе части сравнения $a^{p-1} \equiv 1 \pmod{p}$ на a. Ясно, что получится сравнение, справедливое и при a, кратном p.

Ранее нами рассматривался способ нахождения обратного к заданному числу по некоторому модулю с помощью расширенного алгоритма Евклида. Теорема Эйлера дает нам другой способ решения данной задачи.

Отыскание обратного элемента по теореме Эйлера

Прежде чем находить обратный к заданному необходимо проверить его существование $\exists a^{-1} \bmod n \Leftrightarrow$ НОД(a, n)=1. По теореме Эйлера знаем, если НОД(a, n)=1, то

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

помножим обе части на $a^{-1} \bmod n$ получим [1,3]

$a^{\varphi(n)-1} \equiv a^{-1} \bmod n$

Пример

Найдем $7^{-1} \bmod 10$.

НОД(7,10)=$1 \Rightarrow \exists 7^{-1} \bmod 10$

$\varphi(10) = 4$, теперь

$7^{-1} \equiv 7^3 \bmod 10$

Большое число взять по модулю не всегда просто, поэтому даже при программной реализации в степень возводят постепенно следующим образом. Например нам необходимо получить a в степени n, для этого проделывается следующий алгоритм

0) Result:=1; i:=0;

1) Пока i не равно n делать
2) Result :=Reslt*a mod n;
3) i:=i+1;
4) Перейти на 1)

Теперь по данному алгоритму

$7^2 \equiv 49 \bmod 10 \equiv 9 \bmod 10$

$7^3 \equiv 9 \cdot 7 \bmod 10 \equiv 63 \equiv 3 \bmod 10$

$7^{-1} \equiv 3 \bmod 10$.

Чтоб проверить правильность найденного ответа, необходимо вычислить $a \cdot b \bmod m$, оно по определению должно быть равно 1. $3 \cdot 7 \equiv 1 \bmod 10$.

Ответ: $7^{-1} \equiv 3 \pmod{10}$

Одна из важных задач киптографии - генерация простых чисел, которая состоит из двух частей первая – генерация случайного числа, вторая – проверка этого числа на простоту. Малая теорема Ферма дает нам метод проверки числа на простоту, имеющий одноименное название.

Метод Ферма проверки числа на простоту [6]

Нам необходимо проверить является ли число n простым. По малой теореме Ферма знаем, что для любого простого p, если p не делит a, $a^{p-1} \equiv 1 \pmod{p}$. Поэтому если при одном из значений a данное выражение не выполняется, то есть получается, что $a^{p-1} \neq 1 \pmod{p}$, то число p не простое. Алгоритм можно представить в следующем виде.

1. Повторять t раз (где t параметр надежности)

1.1. Выбрать случайное a такое, что $2 \le a \le n-2$

1.2. Проверить условие: НОД(a, n)=1, если не выполняется, то число составное.

1.3. Вычислить $r = a^{n-1} \bmod n$

1.4. Если $r \neq 1 \bmod n$, то число абсолютно точно является составным

2. Ответ n-простое (с вероятностью близкой к 1 при больших значениях параметра надежности t)

Пример

Проверим на простоту $n=33$

1) Пусть сгенерировалось случайное число $a=10$

$10^{32} \bmod 33 \equiv 1$, возможно простое.

2) Пусть сгенерировалось случайное число $a=23$

$23^{32} \bmod 33 \equiv 1$, возможно простое.

3) Пусть сгенерировалось случайное число $a=6$

$6^{9} \bmod 10 \equiv 3$, абсолютно точно составное.

Ответ: 33 – составное число.

Метод Ферма выполняет задачу когда НОД(a, n) $\neq 1$, обоснуем это. Пусть сгенерировано a такое, что d=НОД(a, n)$\neq 1$, тогда $d|a$ и следовательно $d|a^{n-1}$, так же известно $d|n$. Предположим, что $a^{n-1} \equiv 1 \bmod n$, по (2) записи сравнения $a^{n-1}=1+n \cdot t$ получаем, что $d|1$, чего из начального условия быть не может. Значит наше предположение, что $a^{n-1} \equiv 1 \bmod n$ неверно.

Подытожим, если в шаге 1.1. будет выбрано случайное число a не взаимно простое с n, то метод Ферма сработает точно.

Теперь рассмотрим случай когда выбирается a такое, что НОД(a, n)=1. В данном случае возможно столкновение с псевдослучайными числами или числами Кармайкла.

Определение: Составное число n называется ***числом Кармайкла*** если для любого a, такого что НОД(a, n)=1 выполняется

$a^{n-1} \equiv 1 \bmod n$.

В данном случае возможна ошибка метода Ферма с небольшой вероятностью [5,6]. Минимальное число Кармайкла $561 = 3 \cdot 11 \cdot 17$, как мы видим оно является составным.

Если при проверке данного числа мы выберем a, такое что НОД(a, 561)=1 то по **Лемме 4.1** получаем

НОД(a, 3)=1 по теореме Эйлера $a^2 \equiv 1 \bmod 3 \Rightarrow a^{560} \equiv (a^2)^{280} \equiv 1 \bmod 3$

НОД(a,11)=1 по теореме Эйлера $a^{10} \equiv 1 \bmod 11 \Rightarrow a^{560} \equiv (a^{10})^{56} \equiv 1 \bmod 11$

НОД(a,17)=1 по теореме Эйлера $a^{16} \equiv 1 \bmod 17 \Rightarrow a^{560} \equiv (a^{16})^{35} \equiv 1 \bmod 17$

Из чего по 10 свойству сравнений получаем $a^{560} \equiv (a^{16})^{35} \equiv 1 \bmod 561$.

Поэтому отсев чисел Кармайкла в методе Ферма реализуется за счет условия 1.2, так как метод воспринимает их как простые при условии НОД(a,n)=1. Для данного числа Кармайкла можно рассчитать вероятность ошибки метода Ферма, она равна вероятности того, что t раз выбрано a такое что НОД(a, n)=1. Поскольку все числа равновероятны, воспользуемся формулой

$$p_{\text{ошибки}} = \left(\frac{\varphi(n)}{n} \right)^t,$$

где $\frac{\varphi(n)}{n}$ - вероятность одного выбора числа a взаимно простого с n. Зная что

$$\varphi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2})...(1 - \frac{1}{p_k})$$

$$\frac{\varphi(n)}{n} = (1-\frac{1}{p_1})(1-\frac{1}{p_2})...(1-\frac{1}{p_k})$$

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdot ... \cdot p_k^{e_k}$$

Числа Кармайкла являются достаточно редкими, имеется всего *2163* чисел Кармайкла не превосходящих *25 000 000 000*. До *100 000* числами Кармайкла являются только следующие 16 чисел *561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, 15841, 29341, 41041, 46657, 52633, 62745, 63973,* и *75361*.

Теорема Корселета

Составное *n* есть число Кармайкла если и только если выполняются следующие 2 условия:

1) Не существует таких *p*, что $p^2|n$.

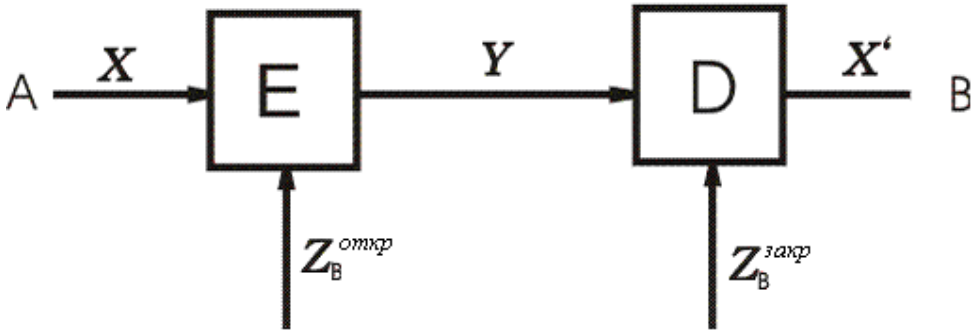
2) Для любого простого *p* такого, что $p|n$ выполняется $(p-1)|(n-1)$.

Проверка того, является ли заданное число числом Кармайкла, согласно данной теореме требует нахождения разложения числа на простые сомножители, т.е. факторизации числа. Поскольку задача факторизации чисел является более сложной, чем задача проверки простоты, то предварительная отбраковка чисел Кармайкла не представляется возможной.

Криптосистема RSA

Самой первой и в то же время самой простой для понимания является криптосистема RSA [5,6], разработанная Роном Ривестом, Ади Шамиром и Леонардом Эдлеманом в 1978 году. Стойкость системы основана на задаче факторизации, то есть на том факте, что легко перемножить два больших простых числа, но очень сложно из полученного произведения восстановить эти числа (участвовавшие в произведении).

Взаимодействие абонентов с помощью криптосистемы с открытым ключом осуществляется следующим образом. Для приема секретного сообщения от абонента А абонент В генерирует два своих ключа $Z_B^{Закр}$ и $Z_B^{Откр}$, закрытый и открытый соответственно. Закрытый ключ хранится в тайне на недоступном носителе, а открытый ключ пересылается предполагаемым абонентам или размещается в сети на доверенном сервере, чтобы его мог получить любой желающий. Для передачи абоненту В сообщения X абонент А шифрует его открытым ключом абонента В $Y=E(X, Z_B^{Откр})$ и передает его по некоторому каналу абоненту В. Последний своим закрытым ключом расшифровывает $X'=D(Y, Z_B^{Закр})$. Расшифровать сообщение зашифрованное с помощью открытого ключа можно только закрытым.



Разберем построение RSA.

1) Сгенерируем p и q — два различных больших случайно выбранных простых числа (имеющих более *100* разрядов в их десятичном представлении или в двоичном представлении $\sim 2^{1024}$).

2) Вычислим $n = pq$ и $\varphi(n) = (p - 1)(q - 1)$.

3) Случайно выберем большое число $d > 1$, такое, что НОД$(d,\varphi(n)) = 1$. и вычислим e, $1<e<\varphi(n)$, удовлетворяющее сравнению $ed = 1 \pmod{\varphi(n)}$.

Числа e и d называются ***экспонентой зашифрования*** и ***расшифрования*** соответственно. Числа n и e образуют ***открытый ключ зашифрования***, тогда как оставшиеся числа p, q, $\varphi(n)$ и d формируют ***секретный ключ***. Очевидно, что секретный ключ включает в себя взаимозависимые величины. К

примеру, зная p, нетрудно вычислить оставшиеся три величины.

4) При зашифровании исходный текст возводится в степень e по модулю n

$y=x^e \bmod n$.

5) При расшифровании криптотекст возводится в степень d по модулю n

$x=y^d \bmod n$.

Поясним шифрование: потребуем, чтобы исходный текст кодировался двоичным числом. Данное число затем делится на двоичные блоки подходящего размера. Каждый блок шифруются отдельно. Их размер определяется как единственное целое число i, удовлетворяющее неравенствам $2^{i-1} < n < 2^i$. В некоторых случаях в качестве размера блоков можно выбрать число $i - 1$, однако, если важна однозначность расшифрования, нужно быть уверенным в том, что каждому блоку соответствует число, меньшее n.

Обоснуем корректность расшифрования, то есть обоснуем равенство $y = x^e \pmod n$.

В силу выбора, d существует положительное целое число t, такое, что $ed = t\cdot\varphi(n) + 1$. Потребуем сначала, чтобы ни p, ни q не делили x. По теореме Эйлера $x^{\varphi(n)} = 1 \pmod n$, откуда $x^{ed-1} = 1 \pmod n$. Следовательно, $y^d = (x^e)^d = x \pmod n$.

Если одно из p и q, скажем p, делит x, то $x = 0 \pmod p$, тогда $x^{p-l} = 0 \pmod p$. Поэтому $x^{ed} = x \pmod n$.

Задания

1.4.1 Вычислить функцию Эйлера

1332	*432*
1776	*576*
1836	*576*
2016	*576*

1.4.2 Вычислить обратное с помощью функции Эйлера

$11^{-1} \bmod 15$	Ответ *11*
$27^{-1} \bmod 30$	Ответ *обратного нет*
$7^{-1} \bmod 10$	Ответ *3*

§II.5. РЕШЕНИЕ СРАВНЕНИЙ ПЕРВОЙ СТЕПЕНИ, ЛИНЕЙНЫЙ КОНГРУЭНТНЫЙ ГЕНЕРАТОР

В следующих пунктах мы будем рассматривать и учиться решать сравнения с одним неизвестным вида

$$f(x) \equiv 0 (\bmod m),$$

где $f(x)=a_n x^n + a_{n-1} \cdot x^{n-1} + ... + a_1 \cdot x + a_0$ - многочлен с целыми коэффициентами. Если m не делит a_n, то говорят, что n - степень сравнения. Ясно, что если какое-нибудь число x подходит в сравнение, то в это же сравнение подойдет и любое другое число, сравнимое с x по модулю m . Решить сравнение - значит найти все те x, которые удовлетворяют данному сравнению, при этом весь класс чисел по модулю m считается за одно решение.

Таким образом, число решений сравнения есть число вычетов из полной системы, которые этому сравнению удовлетворяют.

Начнем со сравнения первой степени

$a \cdot x \equiv b \pmod{m}$, где $a<m$, $b<m$. Или если вас смущает такая запись

$a \cdot x - b \equiv 0 \pmod{m}$

Если x_1 - решение, то все $y \equiv x_1 \pmod{m}$, так же решение уравнения [1,3]. Чтобы упростить ситуацию будем находить решение $1 \le x \le m$ и ответ записывать в виде $[x]$.

1) Пусть НОД$(a, m)=1 \Rightarrow \exists a^{-1} \bmod m$, помножив обе части сравнения на a^{-1}

$a^{-1}a \cdot x \equiv a^{-1}b \pmod{m}$

$x \equiv a^{-1}b \pmod{m}$

Поэтому при НОД$(a,m)=1$, сравнение $a \cdot x \equiv b \pmod{m}$имеет только одно решение:

$x \equiv a^{-1}b \pmod{m}$

Пример

Решим сравнение $3 \cdot x \equiv 2 \pmod{11}$

НОД$(7;10)=1$

$3^{-1} \pmod{11} = 4$

$3^{-1} \cdot 3 \cdot x_1 \equiv 3^{-1} \cdot 2 \pmod{11}$

$x_1 \equiv 8 \pmod{11}$

Ответ: $x = [8]$.

2) Теперь пусть НОД$(a\ m)=d$ отличен от единицы. Тогда предположив, что x_1 - решение, т.е. $a \cdot x_1 = b \pmod{m}$.

$$\left.\begin{array}{l} ax_1 = b + m \cdot t \\ d \mid a \Rightarrow d \mid ax_1 \\ d \mid m \Rightarrow d \mid mt \end{array}\right\} \Rightarrow d \text{ должно делить } b.$$

Пусть $a=a_1 \cdot d$, $b=b_1 \cdot d$ и $m=m_1 \cdot d$, тогда по 9 свойству сравнения обе части

сравнения и модулю можем поделить на их наибольший общий делитель, получим $a_1 \cdot x \equiv b_1 \pmod{m_1}$. Тогда НОД($a_1$,$m_1$)=*1* и данное сравнение можно решить в соответствии с первым пунктом. Оно имеет одно решение

$$x_1 \equiv a_1^{-1} b_1 \pmod{m_1} \qquad (5.1)$$

По исходному модулю *m*, числа (5.1) образуют столько решений исходного сравнения, сколько чисел вида (5.1) содержится в полной системе вычетов: {*0, 1, 2, ..., m-2, m-1*}. Очевидно, что из чисел $x=x_1 + t \cdot m$ в полную систему наименьших неотрицательных вычетов попадают только x_1, x_1+m_1, $x_1 +2 \cdot m_1$, ..., $x_1+(d-1) \cdot m_1$, т.е. всего *d* чисел. Получили, что у исходного сравнения имеется *d* решений.

Подытожим, если НОД(*a*, *m*)=*d*, тогда если *d*|*b*, то сравнение имеет *d* решений:

$x_1, x_1+m_1, x_1 +2 \cdot m_1, ..., x_1+(d-1) \cdot m_1$

где $x_1 = a_1^{-1} b_1 \bmod m_1$ и $m_1 = \frac{m}{d}$, $a_1 = \frac{a}{d}$, $b_1 = \frac{b}{d}$

Пример

$6 \cdot x \equiv 15 \bmod 21$

НОД(*a*,*m*)=НОД(*6, 21*)=*3* (*3* решения), поделим обе части сравнения и модуль на *3*, получим

$2 \cdot x = 5 \bmod 7$

$2^{-1} \bmod 7 = 4$

$x_1 = 20 \bmod 7 = 6$

$x_2 = 6+7 = 13$

$x_3 = 13+7 = 20$

Ответ: {*6,13,20*}.

Линейный конгруэнтный генератор

Одной из важнейших задач криптографии является задача генерации больших простых чисел. Формально данную задачу можно разделить на две:

- задача генерации случайного числа;
- задача проверки числа на простоту.

Рассмотрим задачу генерации чисел [14].

Простейшим и, пожалуй, самым простым генератором псевдослучайных чисел является линейный конгруэнтный генератор

$$xn = (a \cdot xn\text{-}1 + b) \bmod m$$

где x_n - n-ое число в последовательности, а x_{n-1} - предыдущее число последовательности.

Параметры a, b и m - константы. Ключом является начальное значение x_0, например, в языке программирования Pascal (Turbo/Borland Pascal) перед генерацией случайных чисел рекомендуют производить инициализацию генератора (ramdomize;), это и есть инициализация генератора случайных чисел.

ЛКГ имеет период, не превышающий m. Если параметры a, b и m подобраны должным образом, то генератор будет генератором максимального периода с периодом m-1. Для этого, параметр b должен быть взаимно прост с m.

В Таблице, взятой из [15], дается список хороших констант для линейных конгруэнтных генераторов. Приведем часть этой таблицы.

a	*b*	*m*
106	*1283*	*6075*
211	*1663*	*7875*
421	*1663*	*7875*

430	*2531*	*11979*
936	*1399*	*6655*
1366	*1283*	*6075*
171	*11213*	*53125*
859	*2531*	*11979*
419	*6173*	*29282*
967	*3041*	*14406*
141	*28411*	*134456*
625	*6571*	*31104*
1541	*2957*	*14000*
1741	*2731*	*12960*
1291	*4621*	*21870*
205	*29573*	*139968*
421	*17117*	*81000*
1255	*6173*	*29282*
281	*28411*	*134456*

Достоинство ЛКГ в их простоте и нетребовательности к программным ресурсам, но и имеется существенный недостаток – их предсказуемость.

Несколько лучшие результаты показали квадратичный и кубический конгруэнтный генераторы, однако их случайность изначально подвергалась серьезным сомнениям. Джоан Бойяр в [16] восстановила исходную формулу генератора исходя из некоторого диапазона сгенерированных значений. Общие формулы генераторов.

$$x_n = (a \cdot x_{n-1}^2 + b \cdot x_{n-1} + c) \bmod m$$
$$x_n = (a \cdot x_{n-1}^3 + b \cdot x_{n-1}^2 + c \cdot x_{n-1} + d) \bmod m$$

Конечно, реального применения ЛКГ в криптологии, где требования к

случайности генерируемой последовательности достаточно велики, не получили, однако они широко применяются в других задачах.

Задания

1.5.1 Решить сравнения

$7 \cdot x \equiv 4 \bmod 11$	Ответ $x = 10 \bmod 11$
$6 \cdot x \equiv 4 \bmod 27$	Ответ $x = \{7,16,25\}$
$14 \cdot x \equiv 9 \bmod 21$	Ответ *решений нет*
$21x = 15 \bmod 36$	$\{11,23,35\}$
$19x = 12 \bmod 32$	$\{4\}$
$6x = 30 \bmod 18$	$\{5,8,11,14,17,2\}$

§II.6. СРАВНЕНИЕ ЛЮБОЙ СТЕПЕНИ ПО ПРОСТОМУ МОДУЛЮ

В этом пункте мы рассмотрим сравнения вида $f(x) \equiv 0 (\mathrm{mod}\ p)$, где p - простое число, $f(x)=ax^n+a_1x^{n-1}+\ldots+a_n$ - многочлен с целыми коэффициентами, и попытаемся научиться решать такие сравнения [3]. Особенность данного пункта в том, что приводятся некоторые наработки по данному вопросу, но не дается конкретных способов решения, однако это не мешает данному параграфу быть весьма полезным.

Лемма 6.1

Произвольное сравнение $f(x) \equiv 0 \pmod p$, где p - простое число, равносильно некоторому сравнению степени не выше $p-1$.

Доказательство

Разделим $f(x)$ на многочлен x^p-x с остатком: $f(x)=(x^p-x)\cdot Q(x)+R(x)$, где, как известно, степень остатка $R(x)$ не превосходит $p-1$. По теореме Ферма, $x^p-x \equiv 0 (\mathrm{mod}\ p)$. Это означает, что $f(x) \equiv R(x) (\mathrm{mod}\ p)$, а исходное сравнение равносильно сравнению $R(x) \equiv 0 (\mathrm{mod}\ p)$.■

Доказанная лемма дает нам способ сведения сравнений произвольной степени по простому модулю p к сравнению степени не более $p-1$.

Лемма 6.2

Если сравнение $a_nx^n+a_{n-1}x^{n-1}+\ldots+a_0 \equiv 0 (\mathrm{mod}\ p)$ степени n по простому модулю p имеет более n различных решений, то все коэффициенты $a_0,a_1,\ldots,a_n$ кратны p.

Доказательство

Пусть сравнение $ax^n + a_1 x^{n-1} + \ldots + a_n \equiv 0 (\mathrm{mod}\ p)$, имеет $n+1$ решение и x_1, $x_2,\ldots,x_n$, x_{n+1} – наименьшие неотрицательные вычеты этих решений. Тогда, очевидно, многочлен $f(x)$ представим в виде:

$$f(x)=a(x-x_1)(x-x_2)\ldots(x-x_{n-2})(x-x_{n-1})(x-x_n)+$$
$$+b(x-x_1)(x-x_2)\ldots(x-x_{n-2})(x-x_{n-1})+$$
$$+c(x-x_1)(x-x_2)\ldots(x-x_{n-2})+$$
$$+\ldots+$$
$$+\ k(x-x_1)(x-x_2)+$$
$$+l(x-x_1)+$$
$$+m.$$

Действительно, коэффициент b нужно взять равным коэффициенту при x^{n-1} в разности $f(x)-a(x-x_1)(x-x_2)\ldots(x-x_n)$; коэффициент c – это коэффициент перед x^{n-2} в разности $f(x)-a(x-x_1)(x-x_2)\ldots(x-x_n) - b(x-x_1)(x-x_2)\ldots(x-x_{n-1})$, и т.д.

Теперь положим последовательно $x=x_1, x_2,\ldots, x_n, x_{n+1}$. Имеем:

1) $f(x_1)=m \equiv 0 (\mathrm{mod}\ p)$, следовательно, p делит m.
2) $f(x_2)=m+l(x_2 - x_1) \equiv l(x_2 - x_1) \equiv 0 (\mathrm{mod}\ p)$, следовательно, p делит l, ибо p не может делить $x_2 - x_1$, так как $x_2 < p$, $x_1 < p$.
3) $f(x_3) \equiv\ k(x_3 - x_1)(x_3 - x_2) \equiv 0 (\mathrm{mod}\ p)$, следовательно, p делит k.

И т.д.

Получается, что все коэффициенты $a, b, c,\ldots,k, l$ кратны p. Это означает, что все коэффициенты $a_0, a_1,\ldots, a_n$ тоже кратны p, ведь они являются суммами чисел, кратных p. (В этом можно убедится раскрыв скобки в написанном выше разложении многочлена $f(x)$ на суммы произведений линейных множителей). ■

Подведем итог

Всякое нетривиальное сравнение по модулю p равносильно сравнению степени не выше $p-1$ и имеет не более $p-1$ решений.

Как видите, реальных способов решения сравнения по простому модулю мы не получили, однако для небольших p можно воспользоваться процессом перебора всех вычетов из полной системы.

§II.7. РЕШЕНИЕ СИСТЕМ СРАВНЕНИЙ

Основная часть теоремы данного пункта была открыта в первом веке китайским математиком Сун Цзе, она нам дает способ решения систем сравнений [3]. Итак

Китайская теорема об остатках

Пусть $m_1,m_2,\ldots,m_k$ попарно простые числа, тогда система сравнений:

$$\begin{cases} x \equiv b_1 \bmod m_1 \\ x \equiv b_2 \bmod m_2 \\ \quad\quad \ldots \\ x \equiv b_k \bmod m_k \end{cases}$$

Имеем единственное решение $x_1 \pmod m$, где

$m= m_1 \cdot m_2 \cdot \ldots \cdot m_k$,

$$x_1 = \sum_{i=1}^{k} b_i \cdot M_i \cdot M_i'$$

$$M_i = \frac{m}{m_i}$$

$$M_i' = M_i^{-1} \bmod m_i$$

Доказательство

1) Корректность, докажем существование $M_i^{-1} \bmod m_i$. По теореме обратимости обратный существует если и только если НОД(M_i,m_i)=*1*. Как мы знаем

$M_i = m_1 \cdot m_2 \cdot \ldots m_{i-1} \cdot m_{i+1} \ldots \cdot m_k$. Поскольку элементы $m_1,m_2,\ldots,m_k$ попарно просты т.е. НОД(m_i,m_j)=*1* $\forall i \neq j$, а значит (по **Лемме 4.1**) верно и НОД(M_i,m_i)=*1*.

2) Докажем, что для $\forall i$ $x_i \equiv b_i \bmod m_i$, т.е.x_i и есть решение.

Для $\forall i \neq j$ $M_j \equiv 0 \pmod{m_i}$, тогда $x_1 \pmod{m_i} = b_i \cdot M_i \cdot M_i'$, поскольку $M_i' \cdot \equiv M_i^{-1} \pmod{m_i}$, следовательно $M_i \cdot M_i' \equiv 1 \pmod{m_i}$.

3) Докажем единственность решения от противного. Предположим, что их два

x_1 и x_2 – решения, и они не совпадают $x_1 \neq x_2 \pmod{m}$, тогда

$\begin{cases} x_1 \equiv b_i \bmod m_i \\ x_2 \equiv b_i \bmod m_i \end{cases}$, получается $\begin{cases} x_1 \equiv x_2 \bmod m_1 \\ \ldots \\ x_1 \equiv x_2 \bmod m_2 \end{cases}$, по 10 свойству сравнений $\Rightarrow$ $x_1 \equiv x_2 \pmod{m}$ – противоречие. Значит, наше предположение было не верным. То есть решение одно. ■

Пример

Решим систему сравнений вида

$$\begin{cases} x \equiv 1 \bmod 3 \\ x \equiv 2 \bmod 5 \\ x \equiv 5 \bmod 7 \end{cases}$$

m_i	*3*	*5*	*7*
M_i	*35*	*21*	*15*
M_i^{-1}	*2*	*1*	*1*

$M_1' = 35^{-1} \equiv 2^{-1} \bmod 3 = 2$

$M_2' = 21^{-1} \equiv 1^{-1} \bmod 5 = 1$

$M_3' = 15^{-1} \equiv 1^{-1} \bmod 7 = 1$

$x_1 = (35 \cdot 2 \cdot 1 + 21 \cdot 1 \cdot 2 + 15 \cdot 1 \cdot 5) \bmod 105 = 82$

Ответ: [*82*].

Задания

1.7.1 Решить систему уравнений

$\begin{cases} x = 1 \bmod 4 \\ x = 3 \bmod 5 \\ x = 6 \bmod 7 \end{cases}$ Ответ $x=13$

$\begin{cases} x = 2 \bmod 3 \\ x = 4 \bmod 7 \\ x = 3 \bmod 11 \end{cases}$ Ответ $x=179$

$\begin{cases} x = 3 \bmod 6 \\ x = 4 \bmod 7 \\ x = 5 \bmod 10 \end{cases}$ Ответ *решений нет*

§II.8. СРАВНЕНИЕ ВТОРОЙ СТЕПЕНИ

Сравнение второй степени выглядит следующим образом

$$a \cdot x^2 + b \cdot x + c = 0 \pmod m \qquad (8.1)$$

Алгоритм его решения можно представить следующим образом.

$$a \cdot x^2 + b \cdot x = -c \pmod m$$

Введем элемент z следующего вида

$$z = 2 \cdot a \cdot x + b$$

Проделав несложные преобразования, получим

$$z^2 = 4a^2x^2 + 4a \cdot x \cdot b + b^2 = 4a \cdot (a \cdot x^2 + b \cdot x) + b^2 = b^2 - 4 \cdot a \cdot c = D \pmod m$$

$$z^2 \equiv D \bmod m \qquad (8.2)$$

Таким образом, решение сравнения (8.1) сводится к решению сравнения (8.2)

Пример

Решим сравнение первой степени следующего вида

$x^2+2x + 3 = 0 \bmod l7$

$z \equiv 2ax + b = 2x + 2$

$D \equiv 4-4\cdot 3 = -8 = 9 \bmod l7$

$z^2 = 9 \bmod l7$

$z_1 = 3$

$z_2 = -3$

1) $2x + 3 = 3 \bmod l7$

   $2x = l \bmod l7$

   $x_1 = 9 \bmod l7$

2) $2x + 2 = -3 \bmod l7$

   $2x = -5 \bmod l7$

   $x_2 = 6 \bmod l7$

Ответ: $x = \{6, 9\}$

Квадратные вычеты и невычеты

Как мы видим сравнение вида (8.1) свелось к сравнению следующего вида

$$x^2 \equiv a \pmod m \qquad (8.3)$$

Определение: Число a такое, что НОД(a, m)=1 называют квадратным вычетом по модулю m, если сравнение $x^2 \equiv a \pmod m$ имеет хотя бы одно ре-

шение и невычетом в противном случае.

Заметим, что *1* является квадратным вычетом по любому модулю.

Наблюдение 8.1

Пусть p – простое нечетное число (т.е. простое не равное *2*)

a – квадратный вычет по модулю p, тогда сравнение $x^2 \equiv a \pmod m$ имеет ровно *2* решения.

Доказательство

Действительно, если a - квадратичный вычет по модулю p, то сравнение $x^2 \equiv a \pmod p$ имеет хотя бы одно решение $x \equiv x_1 \pmod p$. Тогда $x_2 = - x_1$ – тоже решение, ведь $(-x_1)^2 = x_1^2$. Эти два решения не сравнимы по модулю $p>2$, так как из $x_1 \equiv -x_1 \pmod p$ следует $2x_1 \equiv 0 \pmod p$, т.е. (поскольку $p \neq 2$) $x_1 \equiv 0 \pmod p$, что невозможно, ибо $a \neq 0$.

Докажем, что не $\exists$ решения квадратного сравнения $x_2 \neq \pm x_1 \pmod p$. Пусть $x_2^2 \equiv a \bmod p \Rightarrow x_2^2 \equiv x_1^2 \bmod p \Rightarrow x_2^2 - x_1^2 \equiv 0 \bmod p \Rightarrow$ $p \mid (x_2 - x_1) \vee p \mid (x_2 + x_1) \Rightarrow x_2 \equiv -x_1 \bmod p \vee x_2 \equiv x_1 \bmod p$ чего быть не может. ■

Наблюдение 8.2

Пусть p – простое нечетное, тогда приведенная система вычетов по модулю p содержит $(p-1)/2$ квадратичных вычетов и $(p-1)/2$ квадратичных невычетов.

Доказательство

Выпишем приведенную систему вычетов с ее квадратами

x	*1*	*2*	…	$(p-1)/2$	$(p+1)/2$	…	$p-2$	$p-1$
$x^2 \pmod p$	a_1	a_2	...	a_k	a_k	…	a_2	a_1

$a_1 \equiv 1^2 = (p-1)^2 \pmod p$, т.к. $(p-1) \equiv -1 \pmod p$

$a_2 \equiv 2^2 = (p-2)^2 \pmod p$, т.к. $(p-2) \equiv -2 \pmod p$

…

$a_k \equiv \left(\frac{p+1}{2}\right)^2 = \left(\frac{p-1}{2}\right)^2 \bmod p$, т.к $\frac{p+1}{2} \equiv p - \frac{p-1}{2} \equiv -\frac{p-1}{2} \bmod p$.

Докажем, что $a_i \neq a_j \pmod p$ при $i \neq j$ от противного. Пусть $a_i \equiv k^2 \pmod p$ и $a_j \equiv l^2 \pmod p$

Если $a_i \equiv a_j \pmod p$, тогда по **Наблюдению 8.1** получается, что у каждого сравнения второй степени $x^2 \equiv a_i \equiv a_j \pmod p$ по 4 решения: $\pm k$, $\pm l$. Чего быть не может. ■

Примеры

1) Перечислим все вычеты приведенной системы вычетов по модулю *13*. Для этого построим следующую таблицу. Приведенная система вычетов по модулю *13*: $\mathbf{U_{13}} = \{1,2,3,4,5,6,7,8,9,10,11,12\}$

x	1	2	3	4	5	6	7	8	9	10	11	12
$x^2 \pmod{13}$	1	4	9	3	12	10	10	12	3	9	4	1

Отсюда вычеты {*1, 4, 9, 3, 12, 10*}, все остальные невычеты {*2, 5, 6, 7, 8, 10, 11*}

2) Перечислим все вычеты приведенной системы вычетов по модулю *16*. Построим таблицу. Приведенная система вычетов по модулю *15*: $\mathbf{U_{15}} = \{1,2,4,7,8,11,13,14\}$

x	1	2	4	7	8	11	13	14
$x^2 \pmod{15}$	1	4	1	4	4	1	4	1

Вычетами будут {*1, 4*}, невычетами {*2, 7, 8, 11, 13, 14*}. Такое несоответствие с первой таблицей вызвано тем, что *15* является составным. Таким образом мы хотели обратить ваше внимание на то, что **Наблюдение 8.2** верно при условии простоты модуля.

Символ Лежандра

Начать данный подраздел можно с констатации факта, что фраза «число *a* является квадратичным вычетом/невычетом по *p*» несколько велика, и предложение французского математика Адриена-Мари Лежандра для нас как нельзя кстати. Лежандр предложил следующую формулировку [3].

Определение: Пусть *p* – простое нечетное число, а *a* – любое целое. Тогда символ Лежандра определяется как

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

Данная запись читается как «Символ Лежандра *a* по *p*», или просто «*a* по *p*». Данный символ оказался весьма полезным, далее мы научимся его вычислять.

Теорема (Критерий Эйлера)

Пусть *p* - простое нечетное число, тогда

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

Доказательство

1) Для $p|a$ следует, что $a \equiv 0 \pmod p$, из чего $\left(\frac{a}{p}\right)=a^{\frac{p-1}{2}}=0$.

2) При *a* – квадратичный вычет $\exists\ x$, такой что $x^2 \equiv a \bmod p$, по теореме

Эйлера:

$x^{p-1} \equiv 1 \bmod p$. Из того что НОД(p, a) = 1 (по **Лемме 4.1**) следует НОД(p, x) = 1

$$\left(\frac{a}{p}\right) = x^{p-1} \equiv a^{\frac{p-1}{2}} \equiv 1 \bmod p \qquad (8.4)$$

Квадратных вычетов $\frac{p-1}{2}$, и сравнение $a^{\frac{p-1}{2}} \equiv 1 \bmod p$ имеет не более $\frac{p-1}{2}$ решений, таким образом, все квадратичные вычеты и только они являются решениями сравнения (8.4).

3) Пусть a – квадратичный невычет, тогда по Теореме Эйлера $a^{p-1} \equiv 1 \pmod p$. Можем преобразовать следующим образом $a^{p-1} - 1 \equiv \left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \equiv 0 \bmod p$, тогда $p \mid \left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right)$. И в данной ситуации возможны два варианта:

а) $p \mid \left(a^{\frac{p-1}{2}} - 1\right)$, тогда $a^{\frac{p-1}{2}} \equiv 1 \bmod p$, что не возможно, т.к. a – квадратичный невычет.

б) $p \mid \left(a^{\frac{p-1}{2}} + 1\right)$, тогда $a^{\frac{p-1}{2}} \equiv -1 \bmod p$. Получаем $\left(\frac{a}{p}\right) = -1 = a^{\left(\frac{p-1}{2}\right)} \bmod p$. ■

Приведем некоторые свойства символа Лежандра.

Свойства символа Лежандра

1) Если $a \equiv b \pmod p$, то $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

Это свойство следует из того, что числа одного и того же класса по модулю p будут все одновременно квадратичными вычетами либо квадратичными невычетами. ■

2) $\left(\frac{1}{p}\right)=1$.

Подставим значения в критерий Эйлера, получим искомое выражение. Очевидность доказательства можно подтвердить тем, что единица является квадратным вычетом по любому модулю. ■

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

Доказательство этого свойства следует из критерия Эйлера при $a = -1$. ■

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

Действительно, $\left(\frac{ab}{p}\right)=(ab)^{\frac{p-1}{2}}=a^{\frac{p-1}{2}}b^{\frac{p-1}{2}}=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. ■

5) $\left(\frac{ab^2}{p}\right)=\left(\frac{a}{p}\right)$, т.е. в числителе символа Лежандра можно отбросить любой квадратный множитель. Обоснуем: $\left(\frac{ab^2}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b^2}{p}\right)=\left(\frac{a}{p}\right)\cdot 1=\left(\frac{a}{p}\right)$. ■

Добавим несколько свойств без доказательства.

6) $\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$, проще это свойство можно представить как

$$\left(\frac{2}{p}\right)=\begin{cases}1, \textit{если}\ \ n\equiv 1 \bmod 8\ \ \textit{или}\ \ n\equiv 7 \bmod 8\\ -1, \textit{если}\ \ n\equiv 3 \bmod 8\ \ \textit{или}\ \ n\equiv 5 \bmod 8\end{cases}$$

7) Закон взаимности квадратичных вычетов (Гаусса). Если p и q - нечетные простые числа, то $\left(\frac{p}{q}\right)=(-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{q}{p}\right)$, или иначе

$$\left(\frac{p}{q}\right)=\begin{cases}-\left(\frac{q}{p}\right), \textit{если}\ \ q\equiv p\equiv 3 \bmod 4\\ \left(\frac{q}{p}\right), \textit{если}\ q\equiv 1 \bmod 4\ \textit{или}\ p\equiv 1 \bmod 4\end{cases}$$

Символ Якоби

Якоби Карл Густав Якоб (10.12.1804 - 18.02.1851) - немецкий матема-

тик. Член Берлинской Академии наук. Родился в Потсдаме. В 16 лет поступил в Берлинский университет. Самостоятельно изучал труды Л. Эйлера, П. Лапласа, Ж. Лагранжа и классические языки. В 1825г., защитив диссертацию по вопросу разложения алгебраических дробей на простейшие, получил степень доктора философии. В 1826-1842гг. работал в Кенигсбергском университете, затем принял приглашение на академическую работу в Берлине. Якоби - один из создателей теории эллиптических функций. Он ввел и изучил тета-функции и некоторые другие трансцендентные функции. Применил теорию эллиптических функций к изучению движения волчка, исследованию геодезических линий на эллипсоиде и другим задачам, сделал важные открытия в области теории чисел, линейной алгебры, вариационного исчисления и теории дифференциальных уравнений, в особенности в теории уравнений 1-го порядка (с частными производными; исследовал дифференциальные уравнения динамики и дал ряд новых методов их решения; ввел в употребление функциональные определители и указал на их роль при замене переменных в кратных интегралах и при решении уравнений с частными производными; исследовал один из классов ортогональных многочленов, являющихся обобщением многочленов Лежандра. С именем Якоби связаны теоремы, функции (в частности, тета-функции и эллиптические функции), тождества, уравнения, формулы, интеграл, кривая, матрица, детерминант, радикал, символ.

Умер Якоби в Берлине 18 февраля 1851.

Символ Якоби является обобщением символа Лежандра. Символ Якоби определен для любого целого a и любого n нечетного большего 1, представимого в виде $n=p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_k$, тогда символ Якоби определяется формулой

$$\left(\frac{a}{n}\right)=\left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\ldots\left(\frac{a}{p_k}\right)$$

Свойства символа Якоби

Свойства символа Якоби соответствуют символу Лежандра

1) $\left(\frac{a}{n}\right)=0 \Leftrightarrow$ НОД(a,n)$\neq 1$.

2) Если $a \equiv b \pmod m$, то $\left(\frac{a}{n}\right)=\left(\frac{b}{n}\right)$.

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

4) $\left(\frac{-1}{n}\right)=(-1)^{\frac{n-1}{2}}$.

5) $\left(\frac{1}{n}\right)=1$.

6) $\left(\frac{2}{n}\right)=\begin{cases} 1, если \;\; n \equiv 1 \bmod 8 \;\; или \;\; n \equiv 7 \bmod 8 \\ -1, если \;\; n \equiv 3 \bmod 8 \;\; или \;\; n \equiv 5 \bmod 8 \end{cases}$

7) Закон взаимности квадратичных вычетов(Гаусса). Пусть q, p- положительные, нечетные, взаимно простые, тогда $\left(\frac{p}{q}\right)=(-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{q}{p}\right)$, или иначе

$$\left(\frac{p}{q}\right)=\begin{cases} -\left(\frac{q}{p}\right), \;\; если \;\; q \equiv p \equiv 3 \bmod 4 \\ \left(\frac{q}{p}\right), если\, q \equiv 1 \bmod 4 \, или \, p \equiv 1 \bmod 4 \end{cases}$$

Данные свойства являются следствием записи символа Якоби и в доказательстве не нуждаются. При желании читатель может сам вывести любое.

Пример

Вычислим следующие символы.

$$1)\left(\frac{17}{23}\right)=\left(\frac{23}{17}\right)=\left(\frac{6}{17}\right)=\left(\frac{2}{17}\right)\cdot\left(\frac{3}{17}\right)=\left(\frac{17}{3}\right)=\left(\frac{2}{3}\right)=-1\cdot$$

2) $\left(\frac{21}{29}\right)=\left(\frac{3}{29}\right)^3=\left(\frac{3}{29}\right)=\left(\frac{29}{3}\right)=\left(\frac{2}{3}\right)=-1$.

3) $\left(\frac{18}{43}\right)=\left(\frac{3}{43}\right)^2\left(\frac{2}{43}\right)=\left(\frac{2}{43}\right)=-1$.

4) $\left(\frac{29}{57}\right)=\left(\frac{57}{29}\right)=\left(\frac{28}{29}\right)=\left(\frac{2}{29}\right)^2\left(\frac{7}{29}\right)=\left(\frac{29}{7}\right)=\left(\frac{1}{7}\right)=1$

Задания

1.8.1 Найти все квадратные вычеты по модулю

17	{*1, 2, 4, 8, 9, 13, 15, 16*}
19	{*1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18*}

1.8.2 Вычислить символ Лежандра, с помощью свойств

$\left(\frac{20}{23}\right)$	*-1*
$\left(\frac{29}{43}\right)$	*-1*
$\left(\frac{34}{41}\right)$	*-1*

1.8.3 Вычислить символ Якоби

$\left(\frac{21}{40}\right)$	*1*
$\left(\frac{22}{39}\right)$	*1*

1.8.4 Решить сравнение второй степени

$x^2=20 \bmod 29$	{*7,22*}
$x^2=7 \bmod 31$	{*10,21*}
$3x^2+5x+1=0 \bmod 29$	{*12,25*}
$3x^2+4x-1=0 \bmod 31$	{*13,27*}

$x^2+5x+1=0 \bmod 42 \quad \{15,23\}$

§II.9. РЕШЕНИЕ СРАВНЕНИЙ ПО СОСТАВНОМУ МОДУЛЮ

Теорема 9.1

1) Если числа m_1, m_2,… m_k попарно просты, то сравнение $f(x) \equiv 0 (\bmod m_1 m_2 \dots m_k)$ равносильно системе сравнений:

$$\begin{cases} f(x) \equiv 0 \bmod m_1 \\ f(x) \equiv 0 \bmod m_2 \\ \quad \dots \\ f(x) \equiv 0 \bmod m_k \end{cases} \qquad (9.1)$$

2) При этом, если $T_1, T_2, \dots, T_k$ — числа решений отдельных сравнений этой системы по соответствующим модулям, то число решений T исходного сравнения равно $T_1 T_2 \dots T_k$.(их произведению)

Доказательство

1) Первое утверждение теоремы очевидно, т.к. если $a \equiv b \pmod m$, то $a \equiv b (\bmod d)$, где d делит m . Если же $a \equiv b \pmod{m_1}$ и $a \equiv b \pmod{m_2}$, то $a \equiv b \pmod{\text{НОК}(m_1,m_2)}$, где НОК($m_1$, m_2) – наименьшее общее кратное m_1 и m_2.

2) Каждое сравнение $f(x) \equiv 0 (\bmod m_s)$ выполняется тогда и только тогда, когда выполняется одно из T_s штук сравнений вида $x \equiv b_s \pmod{m_s}$, где b_s пробегает вычеты решений сравнения $f(x) \equiv 0 (\bmod m_s)$. Всего различных комбинаций таких простейших сравнений

$$\begin{cases} x \equiv b_1 \bmod m_1 \\ x \equiv b_2 \bmod m_2 \\ \quad \dots \\ x \equiv b_k \bmod m_k \end{cases} \qquad (9.2)$$

$T_1 T_2 \dots T_k$ штук. Все эти комбинации, по китайской теореме об остатках имеет одно решение. ■

Пример

Решим сравнение

$x^2 \equiv 49 \bmod 55$, по **Теореме 9.1** данное равнение равносильно системе сравнений в соответствии с уравнением (9.1)

$$\begin{cases} x^2 \equiv 49 \bmod 5 \\ x^2 \equiv 49 \bmod 11 \end{cases},$$

решим каждое

1) $x^2 \equiv 49 \bmod 5$

$x_{1,2} \equiv \pm 7 \bmod 5 \equiv \pm 2 \bmod 5$

$\mathbf{B_1}=\{2,3\}$

2) $x^2 \equiv 49 \bmod 11$

$x_{1,2} \equiv \pm 7 \bmod 11$

$\mathbf{B_2}=\{4,7\}$

Составим систему сравнений в соответствии с (9.2)

$\begin{cases} x \equiv b_1 \bmod 5 \\ x \equiv b_2 \bmod 11 \end{cases}$, решим ее в соответствии с китайской теоремой об остатках

m	5	11
M	11	5
M'	1	9

$x \equiv (b_1 \cdot 11 + b_2 \cdot 45) \bmod 55$, где $b_1 \in \mathbf{B_1}$, а $b_2 \in \mathbf{B_2}$

$x_1 \equiv (2 \cdot 11 + 4 \cdot 45) \bmod 55 \equiv 37$

$x_2 \equiv (3 \cdot 11 + 4 \cdot 45) \bmod 55 \equiv 48$

$x_3 \equiv (2 \cdot 11 + 7 \cdot 45) \bmod 55 \equiv 7$

$x_4 \equiv (3 \cdot 11 + 7 \cdot 45) \bmod 55 \equiv 18$

Ответ: $x=\{7, 18, 37, 48\}$.

Задания

1.9.1 Решить сравнения

$x^2=11 \bmod 35$	$\{9,16,19,26\}$
$x^2=19 \bmod 85$	$\{23,28,57,62\}$
$x^2=23 \bmod 143$	$\{32,45,98,111\}$

III. ОСНОВЫ ТЕОРИИ ГРУПП

§III.1. ОСНОВНЫЕ ПОНЯТИЯ

Множество есть совокупность объединенных по некоторым признакам различных объектов, называемых элементами множества.

Примеры множеств

A = {*a*, *b*, *c*}

B = {*x*, *y*}

Поэты = {Пушкин, Есенин, Ахматова, Цветаева, Лермонтов}

Художники = {Айвазовский, Рубенс, Мане, Моне, Ренуар, Ван Дейк}

Если x - элемент множества **X**, то говорят, что x ***принадлежит*** **X**, при этом пишут: $x \in \mathbf{X}$. *В* противном случае делается запись: $x \notin \mathbf{X}$.

Два множества **X** и **Y** ***равны,*** записывается: **X = Y**, если состоят из одних и тех же элементов.

Два множества **X** и **Y** ***не равны***, записывается: $\mathbf{X} \neq \mathbf{Y}$, если найдется элемент одного множества, не являющийся элементом другого множества.

Множество, состоящее из конечного числа элементов, называют ***конечным***, из бесконечного - ***бесконечным.***

Для описания конечного множества **X**, состоящего из элементов $x_1, x_2, \ldots, x_k$ - используется запись

$\mathbf{X} = \{x_1, x_2, \ldots, x_k\}$

порядок следования элементов несущественен.

Число k элементов конечного множества **X** называют ***мощностью*** множества и обозначают через |**X**|.

Для наших множеств

|**A**| = *3*

|**B**| = *2*

|**Поэты**| = *5*

|**Художники**| = *6*

Определение: ***Отображением*** множества **X** в множество **Y** или ***функцией*** *f*, обозначается f: **X→Y,** называется соответствие, определяющее для каждого элемента $x \in$ **X** единственный элемент $y \in$ **Y**. При этом будем писать: $f(x) = y$.

Множество **X** называется ***областью определения*** отображения *f*, множество **Y** - ***областью значений*** отображения *f*, элемент *y* называется ***образом элемента*** *x* относительно отображения *f*, а элемент *x* называется ***прообразом элемента*** *y* относительно отображения *f*.

Пример отображения определенного на **X=Z**, область значений **Y**={*0,1*}

$$f(x) = \begin{cases} 0, & x - четное \\ 1, & x - нечетное \end{cases}$$

А вот например

$$f(x) = \begin{cases} 0, & 2 \mid x \\ 1, & 3 \mid x \end{cases}$$

отображением не является, поскольку для числа *6* существует два элемента из области значений, что противоречит определению.

Задать конечное отображение можно с помощью таблицы либо графом.

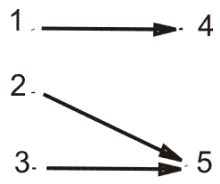
Пример

Продемонстрируем оба вида задания отображения (таблично и графом)

X = {*1,2,3*}, **Y** = {*4,5*}

x	*y*
1	*4*
2	*5*
3	*5*

Таблица



Граф

Отображения *f* и *g* равны**,** если совпадают их области определения и области значений и для любого *x* из области определения.

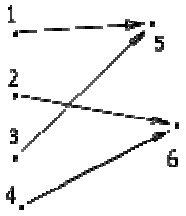
Пусть даны **X** и **Y**, и пусть их мощности |**X**| и |**Y**| соответственно, тогда можем подсчитать |*f*: **X→Y**|, то есть подсчитать количество всевозможных отображений одного множества в другое. Оно будет $|f\colon \mathbf{X}\to\mathbf{Y}| = |\mathbf{Y}|^{|\mathbf{X}|}$, то есть мощность второго в степени мощности первого.

Определение: Отображение *f*:**X→Y** называется ***сюръективным*** или ***отображением на***, если для любого $y\in\mathbf{Y}$ существует $x\in\mathbf{X}$, такое что $f(x)=y$. При этом **|X|≥|Y|.**

Пример сюръективного отображения

x	*y*
1	*5*
2	*6*
3	*5*
4	*6*

Таблично



Граф

Пусть **X** = **Z**(Множество целых чисел), **Y** = **Z** тогда отображение $f(x)=x+1$ является сюръективным. А отображение $f(x)=x^2$ сюръективным на множестве целых чисел не является, поскольку не существует прообраза для, например, *3*.

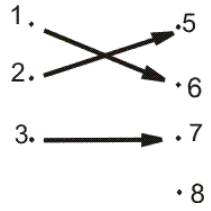
Определение: Отображение *f*: **X→Y** называется ***инъективным***, если из

$x \neq x'$ следует $f(x) \neq f(x')$. При этом $|\mathbf{X}| \leq |\mathbf{Y}|$.

Пример инъективного отображения

x	y
1	*6*
2	*5*
3	*7*
	8

Таблично



Граф

Пусть **X** = **Z** (Множество целых чисел), **Y** = **Z** тогда отображение $f(x)=x+1$ является инъективным. А отображение $f(x)=x^2$ инъективным на множестве целых чисел не является, поскольку для -1 и 1 у нас один прообраз.

Определение: Отображение f: **X**→**Y** называется биективным или ***взаимно-однозначным***, если это отображение одновременно сюръективно и инъективно. Логично, что $|\mathbf{X}|=|\mathbf{Y}|$.

Если даны два отображения f: **X**→**Y** и g: **Y**→**Z**, то ***произведением*** **(*композицией*, *суперпозицией*)** этих отображений называют отображение f: **X**→**Z**, определяемое равенством $h(x) = g(f(x))$, записывается $h=f \cdot g$.

Определение: Отображение e множества **X** в себя называют ***единичным*** **(*тождественным*)**, если $e(x) = x$ для любого $x \in \mathbf{X}$.

Определение: Отображения f:**X**→**Y** и g:**Y**→**X** называют ***взаимно-обратными,*** если $f \cdot g = g \cdot f = e$, при этом пишется: $f^{-1} = g$, $g^{-1} = f$. Отображения, для которых существуют обратные, называются ***обратимыми.*** Отметим, что

Утверждение 1.1

Всякое обратимое отображение имеет единственное обратное отображение.

Утверждение 1.2

Отображение f:**X**→**Y** имеет обратное тогда и только тогда, когда оно биективно. Композиция биективных отображений биективна.

Отображение f:**X**→**X** называют ***преобразованием*** множества **X**.

Определение: Биективное преобразование f n-множества **X** называется ***подстановкой на множестве*** **X,** n **- *степенью подстановки***. Если **X** = {x_1, x_2, ... , x_k}, то f обычно записывают так:

$$f = \begin{pmatrix} x_1 & x_2 & \dots & x_k \\ f(x_1) & f(x_2) & \dots & f(x_k) \end{pmatrix} = \begin{pmatrix} x_1 & x_2 & \dots & x_k \\ x_{i_1} & x_{i_2} & \dots & x_{i_k} \end{pmatrix}$$

здесь (i_1, i_2, ... i_k) перестановка чисел ($1,2,\dots,k$).

$\mathbf{S_n}$-множество всех подстановок степени n.

Несложно подсчитать $|\mathbf{S_n}|=n!$.

Утверждение 1.3

Преобразование обратное подстановке, есть подстановка.

Определим обратную к заданной подстановке на $\mathbf{S_4}$.

$$f = \begin{pmatrix} 1\,2\,3\,4 \\ 2\,1\,3\,4 \end{pmatrix} \qquad\qquad f^{-1} = \begin{pmatrix} 1\,2\,3\,4 \\ 2\,1\,3\,4 \end{pmatrix}$$

Для получения записи подстановки f^{-1} достаточно в записи подстановки f поменять местами верхнюю и нижнюю строки и упорядочить вертикальные пары по элементам верхней строки.

Подстановка f называется ***инволюцией***, если $f^{-1} = f$.

$$g = \begin{pmatrix} 1234 \\ 4123 \end{pmatrix} \qquad g^{-1} = \begin{pmatrix} 1234 \\ 2341 \end{pmatrix}$$

Утверждение 1.4

Композиция подстановок есть подстановка.

$\circ \xrightarrow{f} \circ \xrightarrow{g} \circ$

$a \qquad b \qquad c$

Доказательство: Докажем, что $f \cdot g(x)$ является отображением и биекцией.

1) $\forall a \exists! b : f(a) = b \;\; \forall b \exists! c : g(b) = c \Rightarrow \forall a \exists! c : fg(a) = c \Rightarrow fg(a)$ - отображение

2) $a \neq a'$ (f -инъективно) $\Rightarrow f(a) \neq f(a')$ (g - инъективно)

$\Rightarrow g(f(a)) \neq g(f(a')) \Rightarrow fg$ - инъективно

3) $\forall c \exists b : g(b) = c, (g$ - сюръективно) $\forall b \exists a (f(a) = b) \Rightarrow (gf$ - сюръективно) $\Rightarrow$

$\forall c \exists a g(f(a)) = c \Rightarrow fg$ - сюръективно

Пример

$$f = \begin{pmatrix} 1234 \\ 2143 \end{pmatrix} \qquad g = \begin{pmatrix} 1234 \\ 4123 \end{pmatrix}$$

$$\left.\begin{matrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} \\ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} \end{matrix}\right\} f \circ g \neq g \circ f$$

Некоторые свойства матриц

Определение: Матрицей A размера nxm называется прямоугольная таблица указанного размера, в каждой ячейке которой записан элемент.

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1m} \\ a_{21} & a_{22} & \dots & a_{2m} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nm} \end{pmatrix}$$

Обозначается $A = (a_{ij})$, где a_{ij} есть элемент матрицы A, записанный в i-й строке и j-м столбце, $i = 1, 2,..., n$ и $j = 1, 2,...m$. Если $n = m$, то говорят, что A - квадратная матрица порядка n.

На множестве матриц размера nxm определена операция сложения. Пусть $A = (a_{ij})$, $B = (b_{ij})$, тогда $A+B = (a_{ij} + b_{ij})$, где $a_{ij} + b_{ij}$ - сложение элементов.

Матрицу $A = (a_{ij})$ размера nxm можно умножить на матрицу $B = (b_{ij})$ размера mxr следующим образом

$$A \cdot B = \left(\sum_{k=1}^{m} a_{ik} \cdot b_{kj} \right)$$

Результатом умножения является матрица nxr.

Пусть $\mathbf{M_n}$ - множество всех квадратных матриц порядка n. Единичной матрицей $E = (e_{ij})$ из множества $\mathbf{M_n}$ называется матрица, у которой $e_{11} = e_{22} = ... = e_{nn} = 1$, а остальные элементы равны 0. Для любой матрицы $A \in \mathbf{M_n}$ выполняется: $A \cdot E = E \cdot A = A$.

$$E = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \end{pmatrix}$$

Матрицы $A, B \in \mathbf{M_n}$ называются взаимно-обратными, если $A \cdot B = B \cdot A = E$, при этом матрицу A называют обратной к матрице B (обозначается $A = B^{-1}$) и наоборот. Матрица $A \in \mathbf{M_n}$ называется обратимой, если у нее имеется обратная матрица. Матрица $A \in \mathbf{M_n}$ обратима тогда и только тогда, когда ее определитель не равен 0.

Задания

2.1.1 Определите мощность множеств

A={*1,2,3,4*} *4*

B={*13,11,10*} *3*

A·B *12*

2.1.2 Какие из следующих преобразований являются отображениями, и для являющихся отображениями, определите какими из свойств они обладают (инъективно, сюрьективно, биективно).

$y = x \cdot 2$, определено на **N** ($x,y \in$ **N**)

$y = x/2$, определено на **N**

$y = x^2$, определено на **Z**

$y = x+7$, определено на **Z**

$y = x \bmod 17$, определено на **Z**

2.1.3 Преобразования заданы как

$f(x) = x^2$, определено на **Z**

$g(x) = x+7$, определено на **Z**

$h(x) = x \bmod 17$, определено на **Z**

определить

$f \cdot g$

$g \cdot f$

$f \cdot h$

2.1.4 Определить какие из вышеперечисленных преобразований обратимы.

2.1.5 Определить для заданных подстановок обратные

$f=\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}$ $g=\begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 3 & 1 & 4\end{pmatrix}$ $h=\begin{pmatrix}1 & 2 & 3 & 4\\ 3 & 1 & 4 & 2\end{pmatrix}$

2.1.6 Определить композиции для следующих подстановок, для вышеуказанных матриц

gh

hg

§III.2. ГРУППЫ

Определение: ***Группой*** (**G**, ◦) называется некоторое множество **G** с бинарной операцией ◦ на нем, для которых выполняются следующие четыре условия [2]:

1. Выполняется свойство замкнутости, то есть для любых $a, b \in \mathbf{G}$, $a \circ b \in \mathbf{G}$.

2. Операция ◦ ***ассоциативна***, т. е. для любых $a, b, c \in \mathbf{G}$

$a \circ (b \circ c) = (a \circ b) \circ c$.

3. В **G** существует ***единичный элемент*** (или ***единица***) e, такой, что для любого $a \in \mathbf{G}$

$a \circ e = e \circ a = a$.

4. Для каждого $a \in \mathbf{G}$ существует ***обратный элемент*** $a^{-1} \in \mathbf{G}$, такой, что $a \circ a^{-1} = a^{-1} \circ a = e$.

Если группа удовлетворяет также следующему условию:

5. Для любых $a, b \in \mathbf{G}$

$a \circ b = b \circ a$,

то она называется ***абелевой*** или ***коммутативной***. Первые четыре условия будем называть аксиомами групп.

Иногда запись (**G**, ◦) будем упрощать до **G**.

Отметим, операции сложения и умножения обладают свойством ассоциативности. Группу, на которой введена операция сложения (+) будем на-

зывать аддитивной, умножения (* или ·)- мультипликативной. Мощность множества **G** (количество элементов множества) есть порядок группы, обозначается |**G**|, если порядок конечен, то и группа называется конечной, иначе **G** – группа бесконечного порядка.

Утверждение 2.1

В любой группе нейтральный элемент единственный.

Доказательство

Предположим, что в некоторой группе два нейтральных элемента e_1, и e_2. Тогда уместно следующее $e_1 = e_1 \cdot e_2 = e_2$. Получили $e_1 = e_2$, что и требовалось доказать. ■

Утверждение 2.2

Для любого $a \in \mathbf{G}$ существует единственный обратный элемент.

Доказательство

Пусть для a существует два обратных элемента b, c. Тогда так как $e = a \circ b$ и $e = a \circ c$ по свойству ассоциативности получим

$$b = b \circ (\underbrace{a \circ c}_{e}) = (\underbrace{b \circ a}_{e}) \circ c = c \Rightarrow b = c,$$

то есть $b = c$. ■

Приведем примеры групп

1) (**Z**, +);

- замкнутость выполняется, поскольку сложение двух целых чисел дает целое число;
- операция сложения ассоциативна;
- нейтральный $e = 0$;
- обратный к любому a, будет $-a$, так как $a + (-a) = 0$.

Аддитивная абелева группа, порядок группы бесконечен.

2) Пусть **M**={$2 \cdot a$, $a \in$ **Z**}, тогда группа (**M**, +);

- замкнутость выполняется, т.к. сумма чисел кратных *2* - кратна *2*;
- операция сложения ассоциативна;
- нейтральный $e=0$;
- обратный к a будет $-a$.

Аддитивная абелева группа, порядок группы бесконечен.

3) Пусть **R** – рациональные числа, т.е. все числа вида $\frac{m}{n}$, где $n,m \in$ **Z**. (**R**-**{0}**,$\cdot$) является группой:

- произведение рациональных чисел – рациональное число;
- произведение ассоциативно;
- нейтральный элемент $e=1$;
- обратным к $\frac{m}{n}$ будет $\frac{n}{m}$, здесь становится очевидным, почему мы исключили 0 из множества **R**, мы не можем определить обратный к $\frac{0}{n}$.

Мультипликативная абелева группа, порядок группы бесконечен.

4) ({*1*}, $\cdot$), является простейшим видом группы

- замкнутость выполняется, поскольку произведение единиц даст единицу;
- умножение ассоциативно;
- нейтральный $e=1$;
- обратным к *1* будет *1*.

Мультипликативная абелева группа, порядок группы равен *1*.

По аналогии вы можете заметить, что ({*0*},+) так же является группой.

5) ({*1*,*-1*},$\cdot$) – группа:

- замкнутость выполняется;

- умножение ассоциативно;

- нейтральный $e=1$;

- обратным к 1 будет 1, к -1 будет -1.

Мультипликативная абелева группа, порядок группы равен 2.

6) Полная система вычетов по модулю m ($\mathbf{Z_m}$, $+(\mathrm{mod}\ m)$) так же группа с операцией сложения по модулю

- замкнутость выполняется;

- сложение по модулю ассоциативно;

- нейтральный $e=0$;

- обратным к a будет $(m-a)$;

Аддитивная абелева группа, порядок группы равен m.

7) Приведенная система вычетов по модулю m с операцией модулярного умножения ($\mathbf{U_m}$,$\cdot\ (\mathrm{mod}\, m)$) так же является группой:

- замкнутость выполняется;

- операция модулярного произведения ассоциативна;

- нейтральный элемент $e=1$;

- для каждого элемента полной системы вычетов по определению имеется обратный.

Мультипликативная абелева группа, порядок группы равен $\varphi(m)$.

8) Множество всех подстановок с операцией композиция подстановок ($\mathbf{S_n}$, $\circ$) тоже группа:

- замкнутость выполняется по **Утверждению 1.4**;

- композиция подстановок ассоциативна, и хоть данного утверждения мы не доказывали, это так;

- нейтральный элемент – подстановка вида $e=\begin{pmatrix}1 & 2 & \dots & n\\ 1 & 2 & \dots & n\end{pmatrix}$;

- по **Утверждению 1.3** для любой подстановки можно определить обратную.

Мультипликативная не абелева группа, порядок группы равен $n!$.

9) Пусть дано $\mathbf{M_n}$ множество невырожденных матриц и $\cdot$ - операция матричного умножения, тогда $(\mathbf{M_n},\cdot)$ группа:

- замкнутость выполняется;
- произведение матриц ассоциативно;
- нейтральный элемент $e=E$ - единичная матрица;
- для всякой невырожденной матрицы существует обратная.

Мультипликативная не абелева группа, порядок группы бесконечен.

Существует удобный способ задания конечной группы — в виде таблицы. Эта таблица, представляющая групповую операцию (она обычно называется ***таблицей групповой операции*** или ***таблицей Кэли*** группы), строится так: ее строки и столбцы помечаются элементами группы и на пересечении строки, помеченной элементом a, и столбца, помеченного элементом b, ставится элемент $a \cdot b$.

$\circ$	e	a	b	c	…
e	e	a	b	c	
a	a	$a \circ a$	$a \circ b$	$a \circ c$	
b	b	$b \circ a$	$b \circ b$	$b \circ c$	…
c	c	$c \circ a$	$c \circ b$	$c \circ c$	
…			…		

Пример

Таблица Кэли группы $\mathbf{Z_6}$ имеет вид

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

Отметим, следующие особенности таблицы Кэли

- если группа Абелева, то таблица симметрична относительно главной диагонали,

- в таблице Кэли в каждой строке и каждом столбце все элементы различны и содержатся по одному разу.

Вторую особенность сформулируем в виде утверждения и докажем.

Утверждение

Если в группе **G** $a \neq b$, то $ac \neq bc$.

Доказательство

Пусть $a \neq b$ предположим $a \cdot c = b \cdot c$. По 4-ой аксиоме групп для любого элемента c существует обратный c^{-1} такой, что $c \cdot c^{-1} = e$. Тогда помножим первое равенство на c^{-1}, получим

$a \cdot c = b \cdot c$

$(a \cdot c) \cdot c^{-1} = (b \cdot c) \cdot c^{-1}$ (по 2-ой аксиоме групп)

$a \cdot e = b \cdot e$, то есть $a = b$

Мы пришли к противоречию, следовательно $ac \neq bc$, что и требовалось доказать. ■

Т.е. доказав данное утверждение мы доказали, что все элементы строк и столбца различны. Обратите внимание на предыдущий пример, продемонстрируем данное свойство и на других группах.

Пример

Построим несколько таблиц Кэли. Как уже упоминалось, таблицу мы можем построить только для конечной группы.

1) Построим таблицу Кэли для группы $(\{1,-1\},\cdot\ )$. Таблица будет иметь следующий вид

*	1	-1
1	1	-1
-1	-1	1

2) Построим таблицу Кэли для группы приведенной системы вычетов и операции – сложения по модулю 8 ($\mathbf{U_8},\cdot \pmod 8$). Мощность $\mathbf{U_8}$ равна $\varphi(8)=2^3-2^3=4$.

·	[1]	[3]	[5]	[7]
[1]	[1]	[3]	[5]	[7]
[3]	[3]	[1]	[7]	[5]
[5]	[5]	[7]	[1]	[3]
[7]	[7]	[5]	[3]	[1]

3) Построим таблицу Кэли для следующей группы, подстановка степени 3 с операцией – композиция подстановок ($\mathbf{S_3}$, ○). Сперва перечислим всевозможные подстановки третьей степени. Их всего $|\mathbf{S_n}|=3!=6$ штук:

$$a=e=\begin{pmatrix}123\\123\end{pmatrix}\qquad b=\begin{pmatrix}123\\132\end{pmatrix}\qquad c=\begin{pmatrix}123\\213\end{pmatrix}$$

$$d = \begin{pmatrix} 123 \\ 231 \end{pmatrix} \qquad f = \begin{pmatrix} 123 \\ 312 \end{pmatrix} \qquad g = \begin{pmatrix} 123 \\ 321 \end{pmatrix}$$

○	*e*	*b*	*c*	*d*	*f*	*g*
e	*e*	*b*	*c*	*d*	*f*	*g*
b	*b*	*e*	*d*	*c*	*g*	*f*
c	*c*	*f*	*e*	*g*	*b*	*d*
d	*d*	*g*	*b*	*f*	*e*	*c*
f	*f*	*c*	*g*	*e*	*d*	*b*
g	*g*	*d*	*f*	*b*	*c*	*e*

Простейшие соотношения в группе.

Стандартное обозначение группы имеет следующий вид (**G**, ○), для аддитивной группы будем использовать обозначение (**G**, +), а для мультипликативной (**G**,·).

Закон ассоциативности гарантирует, что выражение вида $a_1 \cdot a_2 \cdot \ldots \cdot a_n$, где $a_i \in \mathbf{G}$, $1 \le i \le n$, не содержит никакой двусмысленности, так как независимо от расстановки скобок это выражение всегда представляет один и тот же элемент группы **G**. Пусть $a \in \mathbf{G}$ и $n \in \mathbf{N}$. Будем применять следующую запись

$a^n = a \cdot a \cdot \ldots \cdot a$ (n сомножителей a)

называя элемент a^n n-ой *степенью* элемента a. Если же групповая операция аддитивна (+), то вместо a^n будем писать

$na = a + a + \ldots + a$ (n слагаемых a).

Для всех $a, b \in \mathbf{G}$ имеет место равенство $(a \cdot b)^{-1} = b^{-1}a^{-1}$, доказательство сего факта следующее. Перемножим $a \cdot b$ с $b^{-1}a^{-1}$, если они взаимнообратны, то их произведение даст нейтральный элемент $(a \cdot b) \cdot (b^{-1}a^{-1}) =$ {по свойству ассоциа-

тивности}=$a(bb^{-1})a^{-1}=e$.

Используя обычные обозначения, мы получаем следующие правила:

	(**G**, +)	(**G**, ·)
e	$e=1$	$e=0$
a^{-1}	a^{-1}	$-a$
	$\underbrace{a\cdot a\cdot a...a}_{n\ раз}=a^n$	$\underbrace{a+a+a+...+a}_{n\ раз}=n\cdot a$
	$\underbrace{a^{-1}\cdot a^{-1}...a^{-1}}_{n раз}=(a^{-1})^n=a^{-n}$	$\underbrace{(-a)+(-a)+...(-a)}_{n раз}=n\cdot(-a)=-n\cdot a$
	$a^n\cdot a^m=a^{n\cdot m}$	$n\cdot a+m\cdot a=a(n+m)$, $n,m\in\mathbf{N}$
	$(a^n)^m=a^{n\cdot m}$	$m\cdot n\cdot a=(m\cdot n)\cdot a$
	$(a\cdot b)^{-1}=b^{-1}\cdot a^{-1}$	$-(a+b)=-b+(-a)$
	$(a^{-1})^{-1}=a$	$-(-a)=a$

Особый интерес представляет группа, в которой каждый элемент является степенью некоторого фиксированного элемента.

Рассмотрим мультипликативную группу следующего вида

G'={…a^{-i}, a^{-i+1},…, a^{-2}, a^{-1}, a^0, a^1, a^2,…, a^i, a^{i+1},…}

Естественен первый вопрос будет ли данная структура группой (**G'**,*). Докажем:

- замкнутость: очевидна,

- ассоциативность: операция умножения ассоциативна,

- нейтральный элемент $e=a^0$,

- для любого a^i обратным будет a^{-i}.

Определение: Мультипликативная группа **G** называется ***циклической***, если в ней имеется такой элемент a, что каждый элемент $b\in$ **G** является сте-

пенью элемента a, т.е. существует целое число k, такое, что $b = a^k$. Этот элемент a называется ***образующим*** группы **G**. Для циклической группы **G** применяют обозначение $\mathbf{G}=\langle a \rangle$.

Из определения следует, что каждая циклическая группа коммутативна. Заметим также, что циклическая группа может иметь не один образующий. Например, в аддитивной группе **Z** образующим является как *1*, так и *-1*., а в группе $(\{1,-1\}, \cdot)$ оба элемента являются образующими.

§III.3. ГРУППЫ СВЯЗАННЫЕ С ШИФРАМИ

Шифром (или криптосистемой) называется совокупность следующих объектов:

- множество сообщений (обычно обозначается **X**);
- множество шифрограмм или зашифрованных сообщений (**Y**);
- множество ключей шифрования ($\mathbf{Z_1}$);
- множество ключей расшифрования ($\mathbf{Z_2}$);
- алгоритм шифрования (E: $\mathbf{X}\cdot\mathbf{Z_1}\rightarrow\mathbf{Y}$, есть ни что иное как отображение);
- алгоритм расшифрования (D: $\mathbf{Y}\cdot\mathbf{Z_2}\rightarrow\mathbf{X}$).

Для любого ключа шифрования принадлежащего множеству ключей шифрования ($z_1\in\mathbf{Z_1}$) существует ключ расшифрования принадлежащий множеству ключей расшифрования ($z_2\in\mathbf{Z_2}$) и для любых сообщения принадлежащих множеству сообщений ($x\in\mathbf{X}$) и любых шифрограмм принадлежащих множеству шифрограмм ($y\in\mathbf{Y}$), если $E(x,z_1)=y$, то $D(y,z_2)=x$. Такая сложная словесная запись весьма компактно записывается математическим языком:

$\forall z_1\in\mathbf{Z_1}\ \exists z_2\in\mathbf{Z_2}\ \forall x\in\mathbf{X}\ \forall y\in\mathbf{Y}$ ($E(x,z_1)=y$, то $D(y,z_2)=x$).

Зачастую алфавиты сообщений и шифртекстов совпадают, для симметричных криптосистем ключи шифрования и рашифрования совпадают, а так же совпадают алгоритмы шифрования и расшифрования.

Приведем примеры некоторых простейших шифров.

Шифр простой замены

Пусть алфавит **А**={*а*, *б*, *в*, *г*, *д*, *е*, *ё*, *ж*, *з*, *и*, *й*, *к*, *л*, *м*, *н*, *о*, *п*, *р*, *с*, *т*, *у*, *ф*, *х*, *ц*, *ч*, *ш*, *щ*, *ъ*, *ы*, *ь*, *э*, *ю*, *я*}.

В данном случае множества сообщений и шифрограмм совпадают (**X**=**Y**) это будет множество слов в алфавите **А**. Ключом является подстановка f:**А**→**А**, в данном случае

$$f = \begin{pmatrix} a_1 & a_2 & \dots & a_{33} \\ a_{i_1} & a_{i_2} & \dots & a_{i_{33}} \end{pmatrix}$$

Каждая буква алфавита заменяется на конкретную другую. Например

$$f = \begin{pmatrix} а & б & \dots & я \\ в & щ & \dots & д \end{pmatrix}$$

При данной подстановке каждая буква *а* исходного текста заменяется на *в*, каждая буква *б* заменяется на *щ*, и т.д. Несложно подсчитать количество возможных ключей или количество всевозможных подстановок. В нашем случае это будет $|f|=33!$, весьма большая величина. Однако вскрывается данный шифр очень просто - частотным методом. Метод основан на том, что каждая буква в тексте встречается с определенной частотой, и если с частотой буквы *а* в шифрограмме встречается, например буква *в*, то, по видимому, произведена именно данная замена (*а* → *в*).

Теперь рассмотрим ситуацию, когда мы, в целях повышения стойкости, шифруем исходное сообщение дважды двумя разными ключами f_1 и f_2 тогда

$$x \xrightarrow{f_1} y \xrightarrow{f_2} y'$$

Композиция подстановок есть подстановка, следовательно, вместо двух подстановок можно было использовать одну другую

$y'=f_2(y)=f_2(f_1(x))= f_1 \circ f_2(x)=f_3(x)$

Поэтому к повышению стойкости двойная подстановка не ведет. Как было ранее доказано композиция подстановок – групповая операция, а само множество подстановок с операцией композицией подстановок - группа, а если шифр образует группу, то их композиция не увеличивает стойкость.

Проще это можно объяснить следующим образом, пусть у нас две подстановки четвертого порядка с алфавитом **А**={*а*, *б*, *в*, *г*}, первая $f_1 = \begin{pmatrix} а & б & в & г \\ б & г & а & в \end{pmatrix}$, вторая $f_2 = \begin{pmatrix} а & б & в & г \\ б & в & а & г \end{pmatrix}$, тогда их композицию можно было заменить одной подстановкой $f_3 = \begin{pmatrix} а & б & в & г \\ в & г & б & а \end{pmatrix}$.

Мы имеем дело с групповой операцией группы ($\mathbf{S_{33}}$, ○{композиция подстановок}).

Шифр перестановки

Аналогично предыдущему шифру, алфавит **А**={*а*, *б*, *в*, *г*, *д*, *е*, *ё*, *ж*, *з*, *и*, *й*, *к*, *л*, *м*, *н*, *о*, *п*, *р*, *с*, *т*, *у*, *ф*, *х*, *ц*, *ч*, *ш*, *щ*, *ъ*, *ы*, *ь*, *э*, *ю*, *я*}. Множества сообщений и шифрограмм совпадают - множество слов в алфавите **А**. Ключом является подстановка f:**А**→**А** произвольного прядка n, тогда объем ключа $n!$. Работает шифр следующим образом, текст разбивается на блоки по n букв

$x=|x_1x_2\ldots x_n|x_{n+1}x_{n+2}\ldots x_{2n}|x_{2n+1}\ldots$

и в каждом блоке переставляются в соответствии с ключом, получаем

$y=|y_1y_2\ldots y_n|y_{n+1}y_{n+2}\ldots y_{2n}|y_{2n+1}\ldots$

Продемонстрируем шифр на примере, пусть ключ подстановка 5 степени

$$f = \begin{pmatrix} 12345 \\ 53421 \end{pmatrix}$$

и пусть сообщение

x=|съешь|_ещё_|этих_|мягки|х_бул|очек_|,

тогда получим следующую шифрограмму

y=|ьешъс|_щёе_|_ихтэ|игкям|лбу_х|_екчо|.

Предположим, что мы хотим повысить стойкость, и дважды шифруем двумя подстановками $f_1 = \begin{pmatrix} 12345 \\ 53421 \end{pmatrix}$ и $f_2 = \begin{pmatrix} 12345 \\ 51234 \end{pmatrix}$, однако их можно было бы заменить одной подстановкой вида $f_3 = \begin{pmatrix} 12345 \\ 42315 \end{pmatrix}$. В данном случае мы имеем дело с композицией подстановок, последняя является операцией группы ($\mathbf{S_5}$, ○{композиция подстановок}). Однако мы можем увеличить стойкость если будем использовать подстановки взаимно простых порядков, поскольку они не будут образовывать группу относительно композиции подстановок.

Вскрытие шифров перестановки производится путем анализа частоты биграмм. ***Биграммой*** будем называть сочетание двух букв алфавита. Например сочетаний вроде фх, щш, шз, сочетаний “гласная”ъ, “гласная”ь, а так же многих других в природе не существует. А у остальных есть некоторая частота появления. Можно, к примеру, написать программу, которая будет перебирать всевозможные подстановки, и проверять на наличие запрещенных биграмм.

Заметим, что для достоверности можно использовать триграммы, тетраграммы и т.д.

§III.4. ПОДГРУППЫ

Порядок элемента.

Мы уже знакомы с понятием порядка группы($\mathbf{G},\circ$), то есть количество элементов множества **G**, теперь мы познакомимся с понятием порядка элемента группы. Суть данных понятий различна, поэтому их следует четко различать [2].

Определение: Наименьшее целое положительное k, такое, что $a^k=1$ (для мультипликативной группы) и $a\cdot k=0$ (для аддитивной группы), называется порядком элемента a, если такого k не существует, то говорят, что a - элемент бесконечного порядка.

Примеры

1) Найдем порядки всех элементов в аддитивной группе ($\mathbf{Z_8}$, +(mod *8*))

a	*0*	*1*	*2*	*3*	*4*	*5*	*6*	*7*
k	*1*	*8*	*4*	*8*	*2*	*8*	*4*	*8*

2) Найдем порядки всех элементов в мультипликативной группе ($\mathbf{U_{15}}$, $\cdot$ (mod *15*))

a	*1*	*2*	*4*	*7*	*8*	*11*	*13*	*14*
k	*1*	*4*	*2*	*4*	*4*	*2*	*4*	*2*

3) Найдем порядки всех элементов в мультипликативной группе ($\mathbf{U_{13}}$, $\cdot \pmod{13}$)

a	1	2	3	4	5	6	7	8	9	10	11	12
k	1	12	3	6	4	12	12	4	3	6	12	2

Обратите внимание, порядки некоторых элементов совпадают с порядком группы, но не один порядок элемента не превосходит порядок группы.

Утверждение 4.1

Если порядок a есть k, то все элементы $a^1,a^2,a^3,\ldots,a^k$ - различны.

Доказательство

Докажем от противного, предположим что в данном ряду $a^1,a^2,a^3,\ldots,a^k$ есть равные $a^i=a^j$ и пусть $i>j$, поскольку $(a^i)^{-1}=(a^j)^{-1}=a^{-j}$,тогда $a^i(a^i)^{-1}= a^i a^{-j} =a^{i-j}=1$. Получили, что $a^{i-j}=1$ и $i-j<k$, чего быть не может так как k-порядок. Следовательно, все элементы $a^1,a^2,a^3,\ldots,a^k$ различны. ■

Утверждение 4.2

Если порядок a есть k и $a^m=1$, то $k|m$ (для мультипликативной группы).

Доказательство

По теореме о делении с остатком $m=k\cdot q+r$, $0\le r<k$, тогда $a^m=a^{k\cdot q+r}=(a^k)^q a^r=a^r=1$. Поскольку $a^r=1$ и $0\le r<k$, значит $r=0$, то есть $m=k\cdot q$. Что по определению делимости значит $k|m$. ■

Подгруппы

Каждая группа содержит некоторые подмножества, которые сами обра-

зуют группу при той же групповой операции. Например, таким свойством обладает подмножество {[*0*], [*2*], [*4*]} группы ($\mathbf{Z_6}$,+(mod *6*))

Определение: Подмножество **H** группы **G** называется ***подгруппой*** этой группы, если **H** само образует группу относительно операции группы **G**. Подгруппы группы **G**, отличные от ***тривиальных подгрупп*** {*e*} и **G**, называется ее ***собственными подгруппами***.

Пример

1) Пусть $\mathbf{M}=\{2\cdot a,\ a\in \mathbf{Z}\}$, **R** – множество рациональных чисел, **C** – множество комплексных чисел, тогда

(**M**,+) подгруппа (**Z**,+)

(**Z**,+) подгруппа (**R**,+)

(**R**,+) подгруппа (**C**,+).

Легко проверяется, что множество всех степеней произвольного элемента *a* группы **G** образует подгруппу этой группы.

Определение. Подгруппа группы **G**, состоящая из всех степеней любого элемента *a* этой группы, называется подгруппой, ***порожденной элементом*** *a*, и обозначается символом $\langle a\rangle$. Эта подгруппа, очевидно, циклическая.

$$\langle a\rangle = \{...,a^{-2},a^{-1},a^{0},a^{1},a^{2},\ldots a^{k},\ldots\}$$

Утверждение 4.3

Если $\langle a\rangle$ - конечная группа, то ее порядок совпадает с ***порядком*** элемента *a*.

Доказательство

Пусть k порядок элемента a, тогда по **Утверждению 4.1** все элементы $a^1,a^2,a^3,\ldots,a^k$ различны. Докажем что при любом m, $a^m \in \{a^1,a^2,a^3,\ldots,a^k\}$. По теореме деления с остатком $m=k\cdot q+r$, $0\le r<k$, $a^m=a^{k\cdot q+r}=(a^k)^q a^r=a^r \in \{a^1,a^2,a^3,\ldots,a^k\}$. Показали что при любом положительном m $a^m \in \{a^1,a^2,a^3,\ldots,a^k\}$. Для любого элемента a^{-m} можно помножив на $k\cdot q$ такое, что $m< k\cdot q$ получим a в положительной степени $a^{k\cdot q-m}$ для которого известно, оно принадлежит $\{a^1,a^2,a^3,\ldots,a^k\}$. ■

Утверждение, имеющее аналогичное доказательство.

Утверждение 4.4

Если $\langle a\rangle$ - конечная подгруппа, то ее порядок совпадает с ***порядком*** элемента a.

Например

Пусть нам дана группа $(\mathbf{U_{15}}, \cdot(\mathrm{mod}\ 15))$, $\mathbf{U_{15}}=\{1,2,4,7,8,11,13,14\}$, элементы и соответствующие им порядки

a	1	2	4	7	8	11	13	14
k	1	4	2	4	4	2	4	2

Элемент *1* имеет порядок *1*, подгруппа {*1*};

Элемент *2* имеет порядок *4*, подгруппа {*2,4,8,1*};

Элемент *4* имеет порядок *2*, подгруппа {*4,1*};

Элемент *7* имеет порядок *4*, подгруппа {*7,4,13,1*};

Элемент *8* имеет порядок *4*, подгруппа {*8,4,2,1*};

Элемент *11* имеет порядок *2*, подгруппа {*11,1*};

Элемент *13* имеет порядок *4*, подгруппа {*13,4,7,1*};

Элемент *14* имеет порядок *2*, подгруппа {*8,4,2,1*}.

Группы, порожденные элементами *2* и *8* совпадают, а так же *7* и *13*.

Разложение группы по подгруппе

Пусть дана некоторая группа **G**, и **H** подгруппа **G**, тогда для любого $x \in \mathbf{G}$ имеют место следующие записи

$x\mathbf{H} = \{x \circ h \mid h \in \mathbf{H}\}$ и $\mathbf{H}x = \{h \circ x \mid h \in \mathbf{H}\}$ называются левым и правым смежными классом группы **G** по подгруппе **H**. Элемент x называется образующим класса.

Например

Пусть нам дана группа ($\mathbf{U_{15}}$, $\circ(\mathrm{mod}\ 15)$), знаем **H**={*1,2,4,8*} является подгруппой заданной группы. Перечислим классы данной группы по подгруппе. Поскольку группа $\mathbf{U_{15}}$ содержит следующие элементы {*1,2,4,7,8,11,13,14*}, то мы должны получить *8* классов.

*1***H** ={*1,2,4,8*}

*2***H** ={*2,4,8,1*}

*4***H** ={*4,8,1,2*}

*7***H** ={*7,14,13,11*}

*8***H** ={*8,1,2,4*}

*11***H** ={*11,7,14,13*}

*13***H** ={*13,11,7,14*}

*14***H** ={*14,13,11,7*}

На самом деле мы получили только *2* класса, классы *1***H** =*2***H** =*4***H** =*8***H**, оказались равными, совпали так же *7***H** =*11***H** =*13***H** =*14***H**.

Свойства классов

Свойства левого и правого классов идентичны [2].

Утверждение 4.5

Если **H** - конечная подгруппа группы **G**, то каждый (левый или правый) смежный класс группы **G** по подгруппе **H** содержит столько же элементов, сколько **H**.

Утверждение 4.6

Пусть $x\mathbf{H}$ смежный класс **G**, тогда $x \in \mathbf{H}$.

Доказательство

Поскольку **H** – подгруппа, то есть она по определению является группой, а значит, в ней есть нейтральный элемент $e \in \mathbf{H}$. А смежный класс получается умножением всех элементов на x, следовательно, в классе будет элемент $xe \in \mathbf{H}$. ■

Утверждение 4.7

Смежный класс порождается любым из своих элементов, т.е. если $y \in x\mathbf{H}$ следовательно $y\mathbf{H} = x\mathbf{H}$.

Доказательство

1) Если $y \in x\mathbf{H}$, то $y=xa$, где $a \in \mathbf{H}$.

Если $z \in y\mathbf{H}$, то $z=yb$, где $b \in \mathbf{H} \Rightarrow z=(xa)b=x(ab)$.

$a,b \in \mathbf{H} \Rightarrow ab \in \mathbf{H}$

$$\left.\begin{array}{l} z=x(ab) \\ ab \in \mathbf{H} \end{array}\right\} \Rightarrow \quad y\mathbf{H} \subseteq x\mathbf{H} \qquad (1)$$

2) Если $y \in x\mathbf{H}$, то $y=xa$, $\Rightarrow x=ya^{-1}$, где $a^{-1} \in \mathbf{H}$.

Если $z \in x\mathbf{H}$, то $z=xb$, $b \in \mathbf{H} \Rightarrow z=(ya^{-1})b=y(a^{-1}b)$.

$a^{-1},b \in \mathbf{H} \Rightarrow a^{-1}b \in \mathbf{H}$

$$\left.\begin{array}{l} z=y(a^{-1}b) \end{array}\right\} \Rightarrow \quad x\mathbf{H} \subseteq y\mathbf{H} \qquad (2)$$

$a^{-1}b \in \mathbf{H}$

из (1) и (2) следует, что $x\mathbf{H}=y\mathbf{H}$. ■

Утверждение 4.8

Если **H** - подгруппа группы **G**, то отношение **ρ** на **G**, определяемое условием

$a\rho b \leftrightarrow a = bh$ для некоторого $h \in \mathbf{H}$,

является отношением эквивалентности.

Вывод

Любые 2 смежных класса группы **G** по подгруппе **H** либо не пересекаются, либо совпадают, т.е. вся группа **G** распадается на множество непересекающихся смежных классов по подгруппе **H**. Множество непересекающихся смежных классов и есть разложение группы по подгруппе **H**.

Пример

Пример разложения группы по подгруппе.

Дана группа ($\mathbf{U_{13}}$, $\cdot (\mathrm{mod}\ 13)$), пусть дана подгруппа $\langle 3\rangle=\{3,9,1\}$

$1\mathbf{H} = \{3,9,1\}$

$2\mathbf{H} = \{6,5,2\}$

$3\mathbf{H} = \{9,1,3\}$

$4\mathbf{H} = \{12,10,4\}$

$5\mathbf{H} = \{2,6,5\}$

$6\mathbf{H} = \{5,2,6\}$

$7\mathbf{H} = \{8,11,7\}$

$8\mathbf{H} = \{11,7,8\}$

$9\mathbf{H} = \{1,3,9\}$

$10\mathbf{H} = \{4,12,10\}$

$11\mathbf{H} = \{7,8,11\}$

$12\mathbf{H} = \{10,4,12\}$

Отметим,

$1\mathbf{H} = 3\mathbf{H} = 9\mathbf{H}$,

$2\mathbf{H} = 5\mathbf{H} = 6\mathbf{H}$,

$4\mathbf{H} = 10\mathbf{H} = 12\mathbf{H}$,

$7\mathbf{H} = 8\mathbf{H} = 11\mathbf{H}$.

Мы разложили группу ($\mathbf{U_{13}}$, $\cdot(\mathrm{mod}\ 13)$) по подгруппе $\langle 3\rangle=\{3,9,1\}$, разложение можно записать в виде $\mathbf{U_{13}}=1\mathbf{H}\cup 2\mathbf{H}\cup 3\mathbf{H}\cup 7\mathbf{H}$.

Определение: Если подгруппа **H** группы **G** такова, что множество смежных классов **G** по **H** конечно, то число этих смежных классов называется ***индексом подгруппы*** **H** в группе **G** и обозначается через (**G:H**).

В приведенном выше примере индекс группы равен *4*, а для разложения ($\mathbf{U_{15}}$,*(mod *15*)) по $\mathbf{H}=\{1,2,4,8\}$ (**G:H**)=*2*.

Теорема Лагранжа

Порядок любой конечной группы равен произведению порядка ее подгруппы на индекс этой подгруппы. Или во всякой конечной группе порядок подгруппы есть делитель порядка группы, т.е. если $|\mathbf{G}|=k$, **H** – подгруппа **G** и $|\mathbf{H}|=m$, тогда (**G:H**)$=k/m$.

Доказательство

Пусть **G** – группа, $|\mathbf{G}|=k$. **H** – подгруппа **G** и $|\mathbf{G}|=m$. Произведем разложение группы G по подгруппе **H**: $\mathbf{G} = 1\mathbf{H}\cup 2\mathbf{H}\cup 3\mathbf{H}\cup s\mathbf{H}$, пусть получилось *s* смежных классов, мощность каждого класса равна мощности подгруппы. |**G**|

$= |\mathbf{H}| \cdot s \Rightarrow m|k$. ■

Следствия теоремы Лагранжа

1. Во всякой конечной группе порядок элемента делит порядок группы.

2. Любая группа простого порядка (порядок p - простое) есть циклическая, причем все элементы отличные от *1* порождающие.

3. Конечная циклическая группа $\langle a \rangle$ порядка m содержит $\varphi(m)$ образующих (т.е. таких элементов a^r, что $a^r = a$). Образующими являются те и только те степени a^r элемента a, для которых НОД(r, m)=*1*.

Задания

2.4.1 Определить порядки элементов в группах

3 в ($\mathbf{Z_{13}}$, +(mod *13*))

4 в ($\mathbf{U_{17}}$, ·(mod *13*))

7 в ($\mathbf{U_{22}}$, ·(mod *22*))

2.4.2 Определить порядки всех элементов в группе ($\mathbf{U_7}$, ·(mod 7))

x	*1*	*2*	*3*	*4*	*5*	*6*
k	*1*	*3*	*6*	*3*	*6*	*2*

($\mathbf{U_{15}}$, ·(mod *15*))

x	*1*	*2*	*4*	*7*	*8*	*11*	*13*	*14*
k	*1*	*4*	*2*	*4*	*4*	*2*	*4*	*2*

$(\mathbf{U_{11}}, \cdot(\mathrm{mod}\ 11))$

x	1	2	3	4	5	6	7	8	9	10
k	1	10	5	5	5	10	10	10	5	2

2.4.3 Разложить группу по подгруппе

$(\mathbf{U_{11}}, \cdot(\mathrm{mod}\ 11))$ по $(<3>, \cdot(\mathrm{mod}\ 11))$ $1\mathbf{H}, 2\mathbf{H}$

$(\mathbf{U_{7}}, \cdot(\mathrm{mod}\ 7))$ по $(<6>, \cdot(\mathrm{mod}\ 7))$ $1\mathbf{H}, 2\mathbf{H}, 3\mathbf{H}$

$(\mathbf{U_{11}}, \cdot(\mathrm{mod}\ 11))$ по $(<10>, \cdot(\mathrm{mod}\ 11))$ $1\mathbf{H}, 2\mathbf{H}, 3\mathbf{H}$

§III.5. ПРИВЕДЕННАЯ СИСТЕМА ВЫЧЕТОВ ПО ПРОСТОМУ МОДУЛЮ

Приведенная система вычетов по простому модулю p содержит все элементы $\{1,2,3,\ldots,p-1\}$, очевидно ее мощность равна $|\mathbf{U_p}| = p-1$. Мы знаем, что $\mathbf{U_p}$ является группой относительно операции умножения по модулю. Однако у нее есть еще одно свойство. Но прежде чем его сформулировать нам потребуется доказать следующую лемму.

Лемма (о порядке произведения)

Пусть $a,b \in \mathbf{G}$, порядком a является r, порядком b – s и НОД$(r,s) = 1$, тогда порядок $a \cdot b$ есть $r \cdot s$.

Доказательство

1) Пусть порядок $a \cdot b$ есть k, тогда вычислим $(ab)^{rs}=(a^r)^s(b^s)^r=e^s e^r=e$, то

есть $k|rs$.

2) Вычислим $(ab)^{rk}=((ab)^k)^r=e^r=e$, т.к. k – порядок ab, но $(ab)^{rk}=((ab)^r)^k=((a)^r(b)^r)^k=b^{rk}=e$, следовательно $s|rk$, а поскольку НОД(s, r) = 1, то $s|k$.

Вычислим $(ab)^{sk}=((ab)^k)^s=e^s=e$, т.к. k – порядок ab, но $(ab)^{sk}=((ab)^s)^k=((a)^s(b)^s)^k=a^{sk}=e$, следовательно $r|sk$, а поскольку НОД(s, r) = 1, то $r|k$.

Из того, что НОД(s;r) = 1, $r|k$ и $s|k$ следует $sr|k$.

$k|rs$ и $sr|k \Rightarrow k=rs$. ■

Теорема (о цикличности U_p)

Пусть p – простое, тогда приведенная система вычетов $\mathbf{U_p}$ – циклическая группа, т.е. в ней существует образующий элемент g порядок которого равен $p-1$, совпадает с порядком группы.

Доказательство

Пусть $p-1=p_1^{e_1}p_2^{e_2}\ldots p_k^{e_k}$ - каноническое разложение, рассмотрим

$$x^{(p-1)/p_1}=1 \bmod p \qquad (5.1)$$

(5.1) имеет $\le (p-1)/p_1 < p$ решений

Выберем b_1 такой, что $b_1^{(p-1)/p_1} \neq 1 \bmod p$

Пусть t – порядок a_1, $a_1 = b_1^{(p-1)/p_1^{e_1}}$

$$\left.\begin{array}{l} a_1^{p_1^{e_1}}=b_1^{p-1}=1 \bmod p \Rightarrow t \mid p_1^{e_1} \\ a_1^{p_1^{e_1-1}}=b_1^{(p-1)/p_1} \neq 1 \bmod p \Rightarrow \neg\, t \mid p_1^{e_1-1} \end{array}\right\} t=p_1^{e_1}$$

для a_1 порядок $p_1^{e_1}$

a_2 порядок $p_2^{e_2}$

…

a_k порядок $p_k^{e_k}$

Тогда $g = a_1 \cdot a_2 \cdot \ldots \cdot a_k$, и порядок g будет равен $p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k} = p\text{-}1 = |\mathbf{U_p}| \Rightarrow g$ – порождающий элемент.

Дискретное логарифмирование

Дискретное логарифмирование [5] основано на факте цикличности приведенной системы вычетов по простому модулю. Пусть p – простое число, тогда приведенная система вычетов $\mathbf{U_p} = \{1, 2, \ldots, p\text{-}1\}$- циклическая группа, то есть существует образующий элемент g, такой, что любой элемент $a \in \mathbf{U_p}$ может быть получен как некоторая степень элемента g. Приведенную систему вычетов можем записать как $\mathbf{U_p} = \{g^1, g^2, \ldots, g^{p-1}\}$.

Определение: Пусть p – простое число, g – образующий элемент группы $\mathbf{U_p}$, любое $a \in \mathbf{U_p}$ $a = g^x \pmod p$, тогда x – дискретный логарифм числа a по основанию g по модулю p, записывается

$x = \log_g a$.

Пример

Пусть $p=13$, порядок $|\mathbf{U_{13}}|=12$.

Из предыдущего примера знаем, образующими группы являются $\{2,6,7,12\}$, построим таблицу дискретных логарифмов по основанию 2.

$\log_2 x$	1	2	3	4	5	6	7	8	9	10	11	12
x	2	4	8	3	6	12	11	9	5	10	7	1

Как мы видим построить данную таблицу не сложно, однако по-

строить обратную к ней затруднительно, но в нашем случае, после предварительной постройки первой уже проще.

x	2	3	4	5	6	7	8	9	10	11	12	1
$\log_2 x$	1	4	2	9	5	11	3	8	10	7	6	12

Задача дискретного логарифмирования, как и задача факторизации, является сложной. Сложность данной задачи основана на том факте, что вычислить $g^k \bmod p = b$ не сложно, однако произвести обратную операцию, для заданного числа b найти степень k, в которой $g^k \bmod p = b$, задача весьма трудоемкая для больших значений p.

Перечислим некоторые свойства логарифмов, которые нам понадобятся в дальнейшем.

Свойства логарифмов

1) Если $a \equiv b \pmod p$, то $\log_g a = \log_g b \pmod{(p-1)}$.

Доказательство

Из условия имеем $a = g^{\log_g a} = b = g^{\log_g b}$, тогда $g^0 = g^{\log_g a - \log_g b} = 1$, следовательно

$(p-1) | (\log_g a - \log_g b)$, из чего, по (3) определению сравнения $\log_g a = \log_g b \pmod{(p-1)}$.■

2) $\log_g(a^n) = n\log_g a$.

3) $\log_g ab = \log_g a + . \log_g b$

Доказательство

Распишем $ab = g^{\log_g a} g^{\log_g b} = g^{\log_g a + \log_g b}$, возьмем логарифм от обеих частей, получим $\log_g ab = \log_g(g^{\log_g a + \log_g b})$, по 2 свойству логарифмов $\log_g ab = \log_g a + . \log_g b$. ■

4) $\log_g a = \log_g d \log_d a \pmod{(p-1)}$

Доказательство

Пусть g, d – образующие элементы $\mathbf{U_p}$. Тогда

$a = d^{\log_d a} = \left[g^{\log_g d}\right]^{\log_d a} = g^{\log_g d \log_d a}$, взяв логарифм от первого и последнего элемента равенства получим исходное выражение. Данное свойство можно использовать в качестве формулы перехода к другому основанию.

Криптосистема Эль-Гамаля

Система Эль-Гамаля [18] – это криптосистема с открытым ключом, основанная на проблеме дискретного логарифмирования. Система включает как алгоритм шифрования, так и алгоритм цифровой подписи.

Система имеет следующие параметры простое число p и g – образующий в группе $\mathbf{U_p}$. Во взаимодействии участвуют два абонента A и B. Принцип взаимодействия абонентов и распространения ключей аналогичен RSA.

Построение

1) Пользователь A генерирует большое простое число p и g образующий в группе $\mathbf{U_p}$.

2) Затем получает секретный ключ a и открытый ключ y, где $y = g^a \pmod{p}$.

3) Секретный ключ хранится на недоступном носителе, открытый размещается на общедоступном доверенном сервере либо рассылается абонентам, от которых ожидается получение шифрованных писем.

4) Пользователь B, желая послать сообщение x пользователю A, сначала выбирает случайное число k, меньшее p. Затем он вычисляет

$y_1 = g^k \pmod{p}$ и

$y_2 = x \oplus (y^k \pmod{p})$,

где ⊕ обозначает побитовое "исключающее ИЛИ"(XOR).

5) После чего B посылает A пару (y_1,y_2)

6) Получив шифрованный текст пользователь A вычисляет $x = (y_1^a \pmod p) \oplus y_2$.

Известен вариант этой схемы, когда операция ⊕ заменяется на умножение по модулю p. Это удобнее в том смысле, что в первом случае текст необходимо разбивать на блоки той же длины, что и число $y^k \pmod p$. Во втором случае этого не требуется и можно обрабатывать блоки текста заранее заданной фиксированной длины (меньшей, чем длина числа p). Уравнение расшифрования в этом случае будет следующим:

$x=y_1^{-a} \cdot y_2 \pmod p$.

Обоснование

Обоснуем шифр следующим образом.

Подставим значения $y_1 = g^k \pmod p$ и $y_2 = x \cdot y^k \pmod p$, в формулу расшифрования получим

$x=y_1^{-a} \cdot y_2 \pmod p=(g^k)^{-a} x \cdot y_1^k \pmod p= g^{-ak} x g^{ak} \pmod p=x \pmod p$.

Итак, мы получили, что обратное шифрованию преобразование (расшифрование) позволяет нам восстановить исходный текст.

Решение сравнений вида $x^n \equiv a \pmod p$, где p - простое

Сравнение вида $x^n \equiv a \pmod p$ по свойствам логарифма можно преобразовать в следующее $n\log_g x \equiv \log_g a \pmod{p-1}$, заменив $\log_g a$ числом, а $\log_g x$ неизвестной получим

$ny \equiv b \pmod{p-1}$, решать подобное сравнение (сравнение первой степени) мы умеем.

Пример

Решим сравнение $x^5 \equiv 7 \pmod{13}$.

x	2	3	4	5	6	7	8	9	10	11	12	1
$\log_2 x$	1	4	2	9	5	11	3	8	10	7	6	12

1) $x^5 \equiv 7 \pmod{13}$

$5\log_2 x \equiv \log_2 7 \pmod{12}$

$5y \equiv 11 \pmod{12}$

$5^{-1} \equiv 5 \pmod{12}$

$y \equiv 5 \cdot 11 \equiv 7 \pmod{12}$

$\log_2 x = 7 \Rightarrow x = 11$

Ответ: $x = 11$.

Задания

2.5.1 Построить таблицу дискретных логарифмов для

$\mathbf{U_7}$ по основанию $g=3$

x	1	2	3	4	5	6
$log_3 x$	0	2	1	4	5	3

$\mathbf{U_7}$ по основанию $g=5$

x	1	2	3	4	5	6
$log_5 x$	0	4	5	2	1	3

$\mathbf{U_{11}}$ по основанию $g=7$

x	1	2	3	4	5	6	7	8	9	1

										0
$log_7 x$	0	3	4	6	2	7	1	9	8	5

U_{13} по основанию $g=2$

x	1	2	3	4	5	6	7	8	9	10	11	12
$log_2 x$	0	1	4	2	9	5	11	3	8	10	7	6

2.5.2 Решить сравнения

$x^5=8 \pmod{13}$ $x=8$

$x^5=4 \pmod{7}$ $x=2$

$x^3=4 \pmod{11}$ $x=5$

$x^{10}=3 \pmod{13}$ $x=\{3,10\}$

IV. КОЛЬЦА И ПОЛЯ

§IV.1. КОЛЬЦА

Определение: ***Кольцом*** (**R**,+,·) называется множество **R** с двумя бинарными операциями, обозначаемыми символами + и ·, такими, что

1. **R** — абелева группа относительно операции +.

2. Операция · ассоциативна, т.е. для всех $a,b,c\in$ **R**

$(a\cdot b)\cdot c = a\cdot(b\cdot c)$.

3. Выполняются ***законы дистрибутивности***, т.е. для всех $a, b, c\in$ **R**

$a\cdot(b+c)= a\cdot b+a\cdot c$ и $(b+c)\cdot a = b\cdot a + c\cdot a$.

Следует обратить внимание на то, что операции + и · не обязательно яв-

ляются обычными сложением и умножением. Для краткости кольцо (**R**,+,·) будем обозначать одной буквой **R**, Единичный элемент аддитивной группы кольца **R** называется ***нулевым элементом*** (или ***нулем***) кольца **R** и обозначается символом *0*, а обратный к элементу *a* этой группы обозначается через -*a*. Вместо *a* + (- *b*) пишут обычно *a* - *b*, а вместо *a*·*b* — просто *ab*. Из определения кольца получается общее свойство *a*·*0* = *0*·*a* = *0* для всех *a*∈**R**. Из этого в свою очередь следует, что (-*a*) *b* =*a*·(-*b*) = -*a*·*b* для всех *a*, *b*∈**R**.

Кольца допускают дальнейшую классификацию, в связи с этим дадим череду определений.

Определение: Кольцо называется ***кольцом с единицей***, если оно имеет мультипликативную единицу, т.е. если существует такой элемент *e*∈**R**, что *ae* = *ea* = *a* для любого *a*∈**R**.

Определение: Кольцо называется ***коммутативным***, если операция · коммутативна.

Определение: Кольцо называется ***целостным кольцом*** (или ***областью целостности***), если оно является коммутативным кольцом с единицей *e*≠*0*, в котором равенство *ab=0* влечет за собой *a=0* или *b=0*.

Определение: Кольцо **R** называется ***телом***, если **R**≠{*0*} и ненулевые элементы в **R** образуют группу относительно операции ·.

Пример

1) (**Z**,+,·) – кольцо, коммутативное с единицей, область целостности, но не тело.

2) (**Z_n**,+mod *n*, · mod *n*) – кольцо, коммутативно с единицей, если *n* простое, то область целостности и тело, если *n* составное – не область целостности и не тело.

3) (**M**{множество квадратных матриц размера *n*x*n*},+,·) с элементами a_{ij} из некоторого кольца **R** – кольцо, коммутативно с единицей, не

область целостности, не тело.

4) ({целые четные},+,·) – кольцо, коммутативно, область целостности, не тело.

Основные соотношения в кольце

1) Для любого $a \in \mathbf{R}$ $0 \cdot a = a \cdot 0 = 0$

2) Если в кольце более одного элемента, то это кольцо с единицей.

3) $(-a)b = a(-b) = -ab$

4) $-(-a) = a$

5) $(-a)(-b) = ab$

6) $(-1)(a) = -a$

Делители нуля

Понятие делителей нуля возникает в ситуации, когда произведение $ab=0$, но $a \neq 0$ и $b \neq 0$. Возникает уместный вопрос, а реальна ли подобная ситуация [2].

Пример

1) В кольце ($\mathbf{Z_{15}}$,+(mod 15),·(mod 15)) числа 3 и 5 являются делителями нуля, т.к. $3 \cdot 5 \equiv 0 (\text{mod } 15)$.

2) В кольце (**M**{множество квадратных матриц размера nxn},+,·) матрицы $\begin{vmatrix} 1 & 0 \\ 0 & 0 \end{vmatrix}$ и $\begin{vmatrix} 0 & 0 \\ 0 & 1 \end{vmatrix}$ являются делителями нуля, т.к. $\begin{vmatrix} 1 & 0 \\ 0 & 0 \end{vmatrix} \cdot \begin{vmatrix} 0 & 0 \\ 0 & 1 \end{vmatrix} = \begin{vmatrix} 0 & 0 \\ 0 & 0 \end{vmatrix}$

Область целостности это ситуация когда отсутствуют делители нуля. Кольцо **R** в котором присутствуют делители нуля будем называть кольцом с делителями нуля.

§IV.2. ПОЛЯ

Коммутативное кольцо называется полем, если его ненулевые элементы образуют группу относительно операции умножения [2]. Иначе говоря,

Определение: полем (**F**,+,·) называется множество **F** элементов, на котором определены операции сложения + и умножения ·, обладающие свойствами:

1. Множество **F** относительно операции сложения является абелевой группой,

2. Множество ненулевых элементов **F**, относительно операции умножения является абелевой группой.

3. Выполняются законы дистрибутивности, т.е. для всех $a, b, c \in \mathbf{R}$
$a\cdot(b+c)= a\cdot b+a\cdot c$ и $(b+c)\cdot a = b\cdot a + c\cdot a$.

Основоположником теории конечных полей является Эварист Галуа.

Эварист Галуа (1811-1832) родился 26 октября 1811г. в городке Бурля-Рен [19]. Его отец Николя - Габриэль Галуа был мэром города. До двенадцати лет Эварист воспитывался в семье, а затем поступил в колледж Луи-ле-Гран. В пятнадцать лет Галуа почувствовал призвание к математике. Он буквально поглощал труды крупных ученых той эпохи: Лежандра, Лагранжа, Гаусса, Коши. С чрезвычайной легкостью он усваивал новый понятия и методы. Начиная с 1829г. его жизнь полна тяжелых испытаний: его отец покончил с собой в результате политической

травли реакционеров, а сам Эварист два раза проваливался при поступлении в Политехническую школу, не пожелав ответить на вопрос, который казался ему лишенным интереса. Он был принят в подготовительную школу, но был исключен из нее в 1831г. из-за своей очень резкой статьи, в которой он разоблачал "реакционные взгляды директора Нормальной школы" во время июльской революции 1830г. Представленные им статьи в Академии два раза были отклонены - в 1829 и 1830 гг. Его третий мемуар "Об условиях разрешимости уравнений в радикалах" был отвергнут Пуассоном в 1831г., так как показался ему не понятным. В нем Галуа разработал основный понятия теории групп для решения до тех пор нерешенных проблем теории уравнений. Лишь в 1843г. благодаря усилиям его друга и его брата Лиувилль, наконец, объявил на заседании Академии о публикации работ Галуа. Она состоялась в 1846г. Однако подлинный смысл теории Галуа во всей полноте был раскрыт только в 1870г. Камилем Жорданом в его "Трактате о подстановках и алгебраических уравнениях".

Галуа страстно поддерживал движение за дело прогресса и революции, возглавляемое Франсуа Распаем и Огюстом Бланки. Все его друзья были убежденными республиканцами. В 1831г. он был арестован за то, что он на многолюдном банкете произнес тост за Луи Филлипа, держа в руке нож. Он был оправдан, но вскоре снова арестован как один из организаторов демонстрации. Заключенный в тюрьму Сен-Пелажи, он продолжал свои исследования, очень много работал над интегралами от алгебраических функций. Здоровье Галуа ухудшилось 16 марта 1832г. он был переведен в лечебницу Фольтрие, где он пользовался некоторой свободой. Именно здесь он познакомился с женщиной, которая сыграла роковую роль в судьбе Эвариста. 29 апреля он выходит на свободу, а через месяц, вследствие какой-то весьма темной истории, он был вынужден драться на дуэли, хотя и приложил все усилия, чтобы добиться примирения. В

ужасную последнюю ночь перед дуэлью Галуа лихорадочно перечитывал все свои статьи и написал свое знаменитое "Письмо к Огюсту Шевалье", ставшее его научным завещанием. В нем он вверял своему другу все свои работы (два мемуара, наброски, черновики), всю эту, по его словам, "кашу, в которой надо разобраться". В письме содержится также классификация абелевых интегралов, к которой заново пришел Риман двадцать пять лет спустя. Утром 30 мая 1832г. какой-то крестьянин около пруда в местечке Жантийи наткнулся на тяжело раненого человека. Раненого человека перевезли в больницу, где он скончался утром следующего дня на руках своего брата.

Свойства полей

1. В поле отсутствуют делители нуля, то есть если $a \cdot b=0$, то $a=0$ или $b=0$.

Доказательство

Пусть $a \cdot b=0$ и $a \neq 0$, тогда для любого отличного от 0 элемента существует обратный a^{-1}, далее

$a^{-1}ab= a^{-1}0$, получим $b=0$. ■

2. $|\mathbf{F}| \geq 2$.

Это условие следствие того, что в поле обязательно должны быть элементы нейтральные по сложению и умножению, то есть 0 и 1, причем $0 \neq 1$.

3. Сформулируем данное свойство в виде теоремы:

Теорема 2.1

Каждое конечное целостное кольцо является полем.

Доказательство: Пусть элементы конечного целостного кольца **R** будут $a_1,a_2,...,a_n$. Для некоторого фиксированного ненулевого элемента $a \in \mathbf{R}$ рассмотрим произведения $aa_1,aa_2,...,aa_n$. Они различны, так как если $aa_i = aa_j$, то $a \cdot (a_t - a_j)=0$, и так как $a \neq 0$, то $a_t=a_j=0$, т.е. $a_t = a_j$. Таким образом, каждый эле-

мент в **R** имеет вид aa_t и, в частности, среди них имеется $e=aa_i$ для некоторого i, $1\le i\le n$, где e - единица **R**. Поскольку кольцо **R** коммутативно, то также $a_ta=e$, так что элемент a_i является мультипликативным обратным к a. Таким образом, ненулевые элементы кольца **R** образуют абелеву группу, тогда **R** - поле. ■

Примеры

1. Множество рациональных чисел **R**.

2. Множество комплексных чисел **C**.

3. Кольцо $(\mathbf{Z_p},+,\cdot)$ Если p - простое, то $\mathbf{Z_p}$ является полем Галуа порядка p и обозначается **GF**(p), *Galua Field*.

§IV.3. ПОДКОЛЬЦА, ИДЕАЛЫ

Определение: Подмножество **S** кольца (**R**,+,·) называется ***подкольцом*** этого кольца, если оно замкнуто относительно операций +, · и образует кольцо относительно этих операций.

Определение: Подмножество **J** кольца **R** называется (***двусторонним***) ***идеалом*** этого кольца, если оно является подкольцом кольца **R** и для всех $a\in\mathbf{J}$ и $r\in\mathbf{R}$ имеет место $ar\in\mathbf{J}$ и $ra\in\mathbf{J}$.

Примеры

1) Пусть **R** - поле рациональных чисел. Тогда множество **Z** целых чисел является его подкольцом, но не идеалом, так как, например, $1\in\mathbf{Z}$, $^1/_2\in\mathbf{R}$, но $^1/_2\cdot 1=\,^1/_2\notin\mathbf{Z}$.

2) $\mathbf{Z_{15}}=\{0,\ldots,14\}$. $(\mathbf{Z_{15}},+(\mathrm{mod}15),\cdot(\mathrm{mod}15))$ - коммутативное кольцо, множество $\{3,6,9,12,0\}$ является подкольцом $\mathbf{Z_{15}}$ и его идеалом.

3) Подкольцо $n\mathbf{Z}$ является идеалом кольца **Z**, поскольку для любого

целого $m \in \mathbf{Z}$ $m(n\mathbf{Z}) \in n\mathbf{Z}$. Факторкольцо $\mathbf{Z}/n\mathbf{Z}$ - это множество вычетов по модулю n с операциями сложения и умножения. Второй пример является частным случаем данной ситуации. Отметим, что если число n не является простым, то $\mathbf{Z}/n\mathbf{Z}$ имеет делители нуля.

Определение: Пусть **R** - коммутативное кольцо. Идеал **J** кольца **R** называется ***главным***, если существует элемент $a \in \mathbf{R}$, такой, что $\mathbf{J}=(a)$. Здесь, для коммутативного кольца **R**, величина $(a)=\{ra+na \mid r \in \mathbf{R},\ n \in \mathbf{Z}\}$ - наименьший идеал, содержащий данный элемент $a \in \mathbf{R}$. Если кольцо имеет единицу, то $(a)=\{ra \mid r \in \mathbf{R}\}$ ((a) - главный идеал). В этом случае **J** называют также главным идеалом, ***порожденным элементом a***.

Во втором примере идеал $\mathbf{J}=\{3,6,9,12,0\}=(3)$ является главным.

Если кольцо **R** является полем, то всякий ненулевой идеал **J** в **R** совпадает со всем полем. В самом деле, если $x \in \mathbf{J}$, $x \neq 0$, то для всякого $y \in \mathbf{R}$ имеем: $(y \cdot x^{-1})x \in \mathbf{J}$, откуда $y \in \mathbf{J}$.

Каждый идеал **J** кольца **R** определяет некоторое разбиение множества **R** на смежные классы по аддитивной подгруппе **J**, называемые ***классами вычетов кольца*** **R** ***по модулю идеала*** **J**. Класс вычетов кольца **R** по модулю **J**, содержащий элемент $a \in \mathbf{R}$, будем обозначать через $[a]=a+\mathbf{J}$, так как он состоит из всех элементов **R** вида $a+c$, где $c \in \mathbf{J}$. Элементы $a,b \in \mathbf{R}$, принадлежащие одному и тому же классу вычетов по модулю **J** (т.е. такие, что $a-b \in \mathbf{J}$), будем называть ***сравнимыми по модулю*** **J** и записывать это так: $a \equiv b \pmod{\mathbf{J}}$. Нетрудно проверить, что если $a \equiv b \pmod{\mathbf{J}}$, то

$$a+r \equiv b+r \pmod{\mathbf{J}},$$
$$ar \equiv br \pmod{\mathbf{J}},$$
$$ra \equiv rb \pmod{\mathbf{J}},$$
$$na \equiv nb \pmod{\mathbf{J}}$$

для любых $r \in \mathbf{R}$ и $n \in \mathbf{Z}$. Если, кроме того, $r \equiv s \pmod{\mathbf{J}}$, то $a+r \equiv b+s \pmod{\mathbf{J}}$

и $ar \equiv bs (\mathrm{mod}\ \mathbf{J})$.

Прямой проверкой показывается, что множество классов вычетов кольца **R** по модулю идеала **J** образует кольцо относительно операций + и ·, определяемых равенствами

$$(a+\mathbf{J})+(b+\mathbf{J}) = (a+b)+\mathbf{J}, \quad (3.1)$$

$$(a+\mathbf{J})\cdot(b+\mathbf{J}) = ab+\mathbf{J}. \quad (3.2)$$

Определение: Кольцо классов вычетов кольца **R** по модулю идеала **J** относительно операций (3.1) и (3.2) называется ***факторкольцом*** кольца **R** по идеалу **J** и обозначается через **R/J.**

Пример

(факторкольцо $\mathbf{Z}/(n)$). Как и в теории чисел обозначим класс вычетов по модулю n ($n \in \mathbf{N}$), содержащий число $a \in \mathbf{Z}$, через $[a]$; этот класс также может быть записан в виде $a+(n)$, где (n) - главный идеал, порожденный числом n. Элементами кольца $\mathbf{Z}/(n)$ являются

$$[0] = 0 + (n)$$

$$[1] = 1 + (n)$$

$$\dots$$

$$[n-1] = n-1 + (n)$$

Теорема 3.1

Факторкольцо $\mathbf{Z}/(p)$ кольца **Z** целых чисел по главному идеалу, порожденному простым числом p, является полем.

Доказательство

В силу **теоремы 2.1** достаточно показать, что $\mathbf{Z}/(p)$ является целостным кольцом. Ясно, что его единицей является $[1]$ и что равенство $[a]\,[b]=[ab]=[0]$

выполняется в том и только том случае, когда $a \cdot b = k \cdot p$ для некоторого целого числа k. Но поскольку p - простое число, то оно делит произведение $a \cdot b$ тогда и только тогда, когда оно делит по крайней мере один из сомножителей. Следовательно, либо $[a]=[0]$, либо $[b]=[0]$, так что кольцо $\mathbf{Z}/(p)$ не имеет делителей нуля. ■

Пример

Пусть $p=5$. Тогда факторкольцо $\mathbf{Z}/(p)$ состоит из пяти элементов $[0]$, $[1]$,$[2]$,$[3]$ и $[4]$. Операции в этом кольце можно задать таблицами (сложения и умножения), аналогичными таблицам Кэли для конечных групп:

+	[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]

Факторкольцо $\mathbf{Z}/(p)$ - первый пример конечного поля, т.е. поля, содержащего конечное число элементов.

Следует предостеречь читателя от ошибочного предположения, что при образовании факторкольца обязательно сохраняются все свойства исходного кольца. Так, например, свойство отсутствия делителей нуля при этом не всегда сохраняется, что видно на примере кольца $\mathbf{Z}/(n)$ при составном натуральном числе n.

Определение: Для простого числа p обозначим через $\mathbf{F_p}$ множество

{*0,1,...,p-1*} целых чисел, и пусть отображение $\varphi:\mathbf{Z}/(p)\to\mathbf{F_p}$ определяется условием $\varphi([a])=a$ для $a=0,1,...,p-1$. Тогда множество $\mathbf{F_p}$ со структурой поля, индуцированной отображением φ, называется ***полем Галуа порядка p*** (часто оно обозначается также символом **GF**(*p*)).

Пример

Очень важным в дальнейшем будет пример конечного поля $\mathbf{F_2}$ второго порядка. Элементами этого поля являются *0* и *1*, и таблицы операций имеют следующий вид:

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

В таком контексте элементы *0* и *1* называются ***бинарными элементами***.

Характеристика кольца (поля)

Если *b* — произвольный ненулевой элемент кольца **Z** целых чисел, то его аддитивный порядок бесконечен, т. е. из $n\cdot b=0$ следует $n=0$. Однако в факторкольце **Z**/(*p*), где *p* - простое число, аддитивный порядок каждого ненулевого элемента *b* равен *p*, т.е. *p* - наименьшее натуральное число, для которого выполняется равенство $p\cdot b = 0$. Это свойство приводит к следующему важному понятию.

Определение: Пусть **R** - произвольное кольцо. Если существует такое натуральное число *n*, что для каждого $r\in\mathbf{R}$ выполняется равенство $nr=0$, то

наименьшее из таких чисел n (скажем, n_0) называется ***характеристикой кольца*** **R**, а само **R** называется ***кольцом характеристики n_0***. Если же таких натуральных чисел n не существует, то **R** называется Кольцом ***характеристики 0***.

Теорема 3.2

Если кольцо $\mathbf{R}\neq\{0\}$ с единицей e и без делителей нуля имеет положительную характеристику n, то n-простое число.

Доказательство

Поскольку кольцо **R** содержит ненулевой элемент, характеристика n этого кольца больше или равна 2. Если n - составное число, то $n=km$, где $k,m\in\mathbf{Z}$, $1<k,m<n$. Тогда $0=ne=(km)e=(ke)(me)$, так что либо $ke=0$, либо $me=0$ (поскольку в **R** нет делителей нуля). Значит, либо $kr=(ke)r=0$ для всех $r\in\mathbf{R}$, либо $mr=(me)r=0$ для всех $r\in\mathbf{R}$, что противоречит определению характеристики n. ■

Следствие

Характеристикой конечного поля является простое число.

Конечное поле $\mathbf{Z}/(p)$ (т.е. $\mathbf{F_p}$), очевидно, имеет характеристику p, в то время как кольцо **Z** целых чисел и поле **R** рациональных чисел имеют характеристику 0. Заметим, что в кольце **R** характеристики 2 имеет место равенство $2a=a+a=0$, откуда следует, что $a=-a$ для всех $a\in\mathbf{R}$.

§IV.4. МНОГОЧЛЕНЫ НАД ПОЛЕМ

В элементарной алгебре рассматриваются выражения вида $a_nx^n + a_1x + ... + a_0$, называемые ***многочленами*** (или ***полиномами***). Здесь a_i называются коэффициентами многочлена и обычно являются действительными или комплексными числами, а x рассматривается как переменная, т.е., подставляя

вместо x произвольное число a, получаем определенное число $a_0 + a_1a + ... + a_na^n$, называемое ***значением многочлена*** при $x = a$. Арифметика многочленов регулируется обычными правилами.

Пусть **R** - произвольное кольцо. Многочленом над **R** называется выражение вида

$$f(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1x + \ldots + a_nx^n,$$

где n — неотрицательное целое число, коэффициенты a_i, $0 \le i \le n$, - элементы кольца **R**, а x – некоторый символ, не принадлежащий кольцу **R**, называемый ***переменной*** (или ***неизвестной***) над **R**. В тех случаях, когда из контекста ясно, какая переменная имеется в виду, мы для обозначения многочлена $f(x)$ будем использовать символ f. Для удобства будем считать, что член a_ix^i с $a_i=0$ не обязательно выписывать [2,8].

Определение: Многочлены

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

над **R** считаются равными тогда и только тогда, когда $a_i = b_i$ для $0 \le i \le n$.

Определение: Определим ***сумму многочленов*** $f(x)=\sum_{i=1}^{n} a_i x^i$ и $g(x)=\sum_{i=1}^{n} b_i x^i$ равенством

$$f(x)+g(x) = \sum_{i=1}^{n} (a_i + b_i) x^i$$

а ***произведение многочленов*** равенством

$$f(x)g(x) = \sum_{k=1}^{m+n} c_k x^k \text{ , где } c_k = \sum_{i+j=k} a_i b_j$$

Не сложно заметить, что множество многочленов с такими операциями образует кольцо:

1. Множество многочленов образуют абелеву группу по сложению

- сумму многочленов мы определили как многочлен, посему замкнутость выполняется.

- сумма ассоциативна.

- определен многочлен, все элементы которого равны нулю, собственно нейтральный элемент по сложению.

- для любого многочлена $f(x)$ можно определить обратный многочлен как $-f(x)$, т.е. многочлен, все коэффициенты которого имеют обратный знак.

2. Операция произведения ассоциативна.

3. Выполняются законы дистрибутивности.

Определение: Кольцо, образованное многочленами над кольцом $(\mathbf{R},+,\cdot)$ называется ***кольцом многочленов*** над **R** и обозначается через $\mathbf{R}[x]$.

Нулевым элементом кольца $\mathbf{R}[x]$ является многочлен, все коэффициенты которого равны 0. Он называется ***нулевым многочленом*** и обозначается через 0.

Определение: Пусть $f(x) = \sum_{i=1}^{n} a_i x^i$ – многочлен над кольцом **R**, не являющийся нулевым. Значит, можно предположить, что $a_n \neq 0$. Тогда a_n называется ***старшим коэффициентом*** многочлена $f(x)$, a_0 - его ***постоянным членом*** и n - ***степенью*** данного многочлена, степень обозначается символом $n=\deg(f(x))=\deg(f)$. Многочлены степени ≤ 0 называются ***постоянными многочленами*** (или ***константами***). Если кольцо **R** имеет единицу 1 и если старший коэффициент многочлена $f(x)$ равен 1, то многочлен $f(x)$ называется

нормированным.

Подсчет старших коэффициентов суммы и произведения двух многочленов приводит к следующему результату.

Теорема 4.1

Пусть $f,g \in \mathbf{R}[x]$. Тогда

$$\deg(f+g) \le \max(\deg(f), \deg(g)),$$

$$\deg(fg) \le \deg(f)+\deg(g).$$

Если **R** - целостное кольцо, то

$$\deg(fg)=\deg(f)+\deg(g).$$

Аналогичным образом можно определить многочлен над полем, формулы и основные понятия для многочленов над кольцом и полем совпадают. Однако отметим, что множество многочленов над полем является кольцом. Поясним, когда мы говорим «многочлен над полем» мы подразумеваем, что его коэффициенты принимают значения данного поля и между коэффициентами выполняются операции присущие данному полю. Когда же мы говорим «множество многочленов над полем образует кольцо» мы считаем каждый многочлен из данного множества элементом кольца, т.е данное множество (множество многочленов) образует кольцо.

Пусть **F** обозначает поле (не обязательно конечное). Понятие делимости применительно к кольцу многочленов над полем (обозначается $\mathbf{F}[x]$) вводится следующим образом.

Определение: Будем говорить, что многочлен $g \in \mathbf{F}[x]$ делит многочлен $f \in \mathbf{F}[x]$ (записывается $g|f$), если существует многочлен $h \in \mathbf{F}[x]$, такой, что $f=gh$.

В этом случае будем говорить, что многочлен g - ***делитель*** f, а многочлен f ***кратен*** g. Обратимыми элементами в кольце $\mathbf{F}[x]$ являются делители постоянного многочлена 1, а следовательно, ими являются все ненулевые постоянные многочлены и только они.

Как и в кольце целых чисел($\mathbf{Z}$), в кольце многочленов над полем существует деление с остатком.

Теорема(деления многочленов с остатком)

Пусть $g\neq 0$ многочлен из $\mathbf{F}[x]$, где $\mathbf{F}$ – поле, тогда для каждого $f\in\mathbf{F}[x]$ существуют такие многочлены q, $r\in\mathbf{F}[x]$, что

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

Пример

Разделим многочлен $f(x)=x^6+4x^5+3x^4+2x^3+x+4$ на $g(x)=x^2+2x+4$, многочлены определены над полем $\mathbf{Z}_5[x]$.

Произведем деление многочленов, используя обычное деление уголком, используемое в начальной школе.

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

Получили $q(x) = x^4 + 2x^3 + 4x + 2$, $r(x) = x + 1$, и, очевидно, $\deg(r) < \deg(g)$.

Теорема 4.2

Пусть $f_1,..., f_n$ - многочлены из $\mathbf{F}[x]$, не все равные 0. Тогда существует однозначно определенный нормированный многочлен $d \in \mathbf{F}[x]$, обладающий следующими свойствами:

1) d делит каждый многочлен f_i $1 \le i \le n$;

2) любой многочлен $g \in \mathbf{F}[x]$, который делит каждый из многочленов f_i, $1 \le i \le n$, делит и многочлен d.

Нормированный многочлен d, называется ***наибольшим общим делителем*** многочленов $f_1,..., f_n$ и обозначается НОД($f_1,..., f_n$). Если НОД($f_1 ..., f_n$)=1, то многочлены $f_1,..., f_n$ называются ***взаимно простыми***. Они называются ***попарно простыми***, если НОД(f_i, f_j) = 1 для $1 \le i < j \le n$.

Наибольший общий делитель двух многочленов f и g из $\mathbf{F}[x]$ можно найти при помощи алгоритма Евклида [2,8]. Пусть многочлен g отличен от нуля и не делит многочлен f. Тогда

$$
\begin{aligned}
f &= gq_1 + r_1 && 0 \le \deg(r_1) < \deg(g) \\
g &= r_1q_2 + r_2 && 0 \le \deg(r_2) < \deg(r_1) \\
r_1 &= r_2q_3 + r_3 && 0 < \deg(r_3) < \deg(r_2) \\
r_2 &= r_3q_4 + r_4 && 0 \le \deg(r_4) < \deg(r_3)
\end{aligned}
$$

…

$$
\begin{aligned}
&r_{n-3} = r_{n-2}q_{n-1} + && 0 \leq \deg(r_{n-1}) < \deg(r_{n-2})\\
&r_{n-1} && 0 \leq \deg(r_n) < \deg(r_{n-1})\\
&r_{n-2} = r_{n-1}q_n + r_n && \deg(r_{n+1}) = 0\\
&r_{n-1} = r_n q_{n+1}
\end{aligned}
$$

Здесь $q_1, \ldots, q_{n+1}$ и $r_1, \ldots, r_n$ — многочлены из $\mathbf{F}[x]$. Так как степень $\deg(g)$ конечна, то процедура должна закончиться после конечного числа шагов. Если старший коэффициент последнего ненулевого остатка r_n равен b, то $\text{НОД}(f,g)=b^{-1}r_n$.

Для нахождения $\text{НОД}(f_1,\ldots, f_n)$ при $n>2$ и при ненулевых многочленах f_t сначала определяют $\text{НОД}(f_1, f_2)$, а затем последовательно находят, применяя алгоритм Евклида, $\text{НОД}(\text{НОД}(f_1, f_2), f_3) = \text{НОД}(f_1, f_2, f_3)$ и т.д.

Пример

Применим алгоритм Евклида к многочленам
$f(x)=x^6+ 3x^5+ 2x^4+ 4x^3+ 4x^2+ 3x$ и $g(x) = x^3+ 3x^2+ 2x+ 3$ из $\mathbf{Z_5}[x]$, получаем

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

$$
\begin{array}{l|l}
x^3 +3x^2 +2x +3 & x^2+ x+ 2\\
\cline{2-2}
\end{array}
$$

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

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

Или

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

$$x^3+3x^2+2x+3=(x^2+x+2)(x+2)+3x+4$$

$$x^2+x+2=(3x+4)(2x+3)+3$$

$$\text{НОД}(f,g)=b^{-1}\cdot 3=2\cdot 3=1 \pmod 5$$

НОД $(f,g)=1$, т. е. многочлены f и g взаимно просты.

Как мы помним из теории чисел, двойственным к понятию наибольшего общего делителя является понятие наименьшего общего кратного.

Определение: Пусть $f_1,\ldots, f_n$ - ненулевые многочлены из $\mathbf{F}[x]$. Тогда можно показать, что существует однозначно определенный нормированный многочлен $m\in\mathbf{F}[x]$, обладающий следующими свойствами:

1) m делится на каждый многочлен f_i $1\le i\le n$,

2) любой многочлен $g\in\mathbf{F}[x]$, который делится на каждый из многочленов f_i $1\le i\le n$, делится на m. Многочлен m называется ***наименьшим общим кратным*** многочленов $f_1,\ldots, f_n$ н обозначается НОК$(f_1,\ldots, f_n)$. Для двух ненулевых многочленов $f,g\in\mathbf{F}[x]$ имеет место соотношение

$$\text{НОК}(f,g)=\frac{a^{-1}fg}{НОД(f,g)},$$

где a - старший коэффициент произведения fg.

Для трех и более многочленов прямого аналога данной формулы не существует. В этом случае для нахождения наименьшего общего кратного применяется тождество

$$\text{НОК}(f_1,\ldots,f_n)=\text{НОК}(\text{НОК}(f_1,\ldots,f_{n-1}),f_n).$$

В теории конечных многочленов над полем существует понятие схожее с простым числам в теории чисел. Простые элементы кольца $\mathbf{F}[x]$ обычно называются ***неприводимыми многочленами***. Ввиду особой важности этого понятия дадим его определение.

Определение: Многочлен $f\in\mathbf{F}[x]$ называется ***неприводимым над полем*** **F** или в ***кольце*** $\mathbf{F}[x]$, если он имеет положительную степень и равенство $f=gh$, $g,h\in\mathbf{F}[x]$, может выполняться лишь в том случае, когда либо g, либо h является постоянным многочленом. Многочлен положительной степени из $\mathbf{F}[x]$, не являющийся неприводимым над **F**, называется ***приводимым над*** **F**. Приводимость или неприводимость данного многочлена существенно зависит от того, над каким полем он рассматривается.

Например, многочлен $x^2-2\in\mathbf{R}[x]$ неприводим над полем **R** рациональных чисел, но приводим над полем **R** действительных чисел, так как $x^2-2=(x-\sqrt{2})(x+\sqrt{2})$.

Неприводимые многочлены играют важную роль в устройстве кольца $\mathbf{F}[x]$, поскольку каждый многочлен из $\mathbf{F}[x]$ может быть записан и притом единственным способом в виде произведения неприводимых многочленов. Введем аналог основной теоремы арифметики.

Теорема (об однозначном разложении на множители)

Каждый многочлен положительной степени $f\in\mathbf{F}[x]$ (где **F** - поле) может

быть представлен в виде произведения

$$f = af_1^{e_1} f_2^{e_2} \dots f_k^{e_k},$$

где $a \in \mathbf{F}$, $f_1,\dots, f_k$ - различные нормированные неприводимые многочлены из $\mathbf{F}[x]$, а $e_1, e_2 \dots, e_k$ - натуральные числа. Это разложение однозначно с точностью до порядка сомножителей.

Данное разложение будем называть ***каноническим разложением*** многочлена f в кольце $\mathbf{F}[x]$.

Основным вопросом для многочленов из $\mathbf{F}[x]$ является вопрос о том, приводим или неприводим данный многочлен над полем $\mathbf{F}$. Для наших целей особенно интересны многочлены, неприводимые над простым полем $\mathbf{Z_p}$. Чтобы найти все неприводимые нормированные многочлены данной степени n над полем $\mathbf{Z_p}$, можно сначала найти все приводимые нормированные многочлены степени n над этим полем, а затем исключить их из множества всех нормированных многочленов степени n над $\mathbf{Z_p}$. Однако, если числа p или n велики, такой метод непригоден, и для таких случаев существуют более мощные методы.

Пример

Найдем все неприводимые многочлены степени 4 над полем $\mathbf{F_2}$ (заметим, что каждый ненулевой многочлен из $\mathbf{F_2}[x]$ автоматически нормирован). Сперва перечислим все младшие нормированные многочлены кроме постоянных.

1. Можно отметить, что все многочлены первой степени неприводимы, поэтому $x, x+1$.

2. Всего возможно 2^2 многочленов второй степени: x^2, x^2+1, x^2+x, x^2+x+1. Среди них неприводимым является только последний, поскольку остальные могут быть представлены через x, $x+1$: $x^2=x\cdot x$, $x^2+1=(x+1)(x+1)$, $x^2+x=(x+1)x$.

3. Третьей степени возможно 2^3 многочленов: x^3, x^3+x^2,

$x^3+x^2+x+1=(x^2+1)(x+1)$, x^3+x^2+1, x^3+x+1, x^3+x, $x^3+1=(x+1)(x^2+x+1)$, x^3+x^2+x. Неприводимы x^3+x^2+1, x^3+x+1.

4. Всего над полем $\mathbf{F_2}[x]$ возможно 2^4 многочленов: x^4, $x^4+1=(x+1)(x^3+x^2+x+1)$, x^4+x, x^4+x+1, x^4+x^2, $x^4+x^2+1=(x^2+x+1)(x^2+x+1)$, x^4+x^2+x, $x^4+x^2+x+1=(x^3+x^2+1)(x+1)$, x^4+x^3, x^4+x^3+1, x^4+x^3+x, $x^4+x^3+x+1=(x+1)(x^3+1)$, $x^4+x^3+x^2$, $x^4+x^3+x^2+1=(x+1)(x^3+x+1)$, $x^4+x^3+x^2+x$, $x^4+x^3+x^2+x+1$. Очевидно неприводимыми будут x^4+x+1, x^4+x^3+1, $x^4+x^3+x^2+x+1$.

Теорема 4.3

Пусть $f\in\mathbf{F}[x]$. Для того чтобы факторкольцо $\mathbf{F}[x]/(f)$ было полем, необходимо и достаточно, чтобы многочлен f был неприводим над полем $\mathbf{F}$.

Остановимся подробнее на строении факторкольца $\mathbf{F}[x]/(f)$, где f - произвольный ненулевой многочлен из $\mathbf{F}[x]$. Это факторкольцо состоит из классов вычетов $[g]=g+(f)$, где $g\in\mathbf{F}[x]$, а операции вводятся формулами (3.1) и (3.2). Два класса вычетов $g+(f)$ и $h+(f)$ совпадают в том и только том случае, когда $g=h(\mathrm{mod}\ f)$, т.е. когда многочлен $g-h$ делится на f. Это равносильно требованию, чтобы g и h давали один и тот же остаток при делении на f. В классе вычетов $g+(f)$ содержится единственный многочлен $r\in\mathbf{F}[x]$, для которого $\deg(r)<\deg(f)$, этот многочлен просто является остатком при делении g на f. Процесс перехода от f к r называется ***приведением по модулю f***. Единственность многочлена r вытекает из того, что если существует многочлен $r_2\in g+(f)$. такой, что $\deg(r_2)<\deg(f)$, то разность $r-r_2$ должна делиться на f, но поскольку $\deg(r-r_2)<\deg(f)$, то это возможно лишь при $r_2=r$. Различные элементы, образующие факторкольцо $\mathbf{F}[x]/(f)$, можно теперь описать явно: а именно это классы вычетов $r+(f)$, где r пробегает все многочлены из $\mathbf{F}[x]$ степени, меньшей чем $\deg(f)$. Таким образом, если $\mathbf{F}=\mathbf{F_p}$ и $\deg(f)=n\geq 0$, то число элементов факторкольца $\mathbf{F_p}[x]/(f)$ равно числу многочленов степени, меньшей n, в кольце $\mathbf{F_p}[x]$, т.е. p^n.

Примеры

1) Пусть $f(x)=x\in \mathbf{F_2}[x]$. В этом случае $p^n=2^1$ многочленов степени, меньшей *1*, из $\mathbf{F_2}[x]$ определяют полный набор классов вычетов, составляющих факторкольцо $\mathbf{F_2}[x]/(x)$, так что это факторкольцо состоит из классов вычетов $[0]$ и $[1]$.

2) Пусть $f(x)=x^2+x+1\in \mathbf{F_2}[x]$. В этом случае факторкольцо $\mathbf{F_2}[x]/(f)$ состоит из $p^n=2^2$ элементов $[0],[1],[x],[x+1]$. Для построения таблиц сложения и умножения этого факторкольца нужно произвести требуемые операции над многочленами, определяющими соответствующие классы вычетов, а затем, если нужно, привести результаты по модулю f. Мы получаем следующие таблицы:

+	$[0]$	$[1]$	$[x]$	$[x+1]$
$[0]$	$[0]$	$[1]$	$[x]$	$[x+1]$
$[1]$	$[1]$	$[0]$	$[x+1]$	$[x]$
$[x]$	$[x]$	$[x+1]$	$[0]$	$[1]$
$[x+1]$	$[x+1]$	$[x]$	$[1]$	$[0]$

·	$[0]$	$[1]$	$[x]$	$[x+1]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[x]$	$[x+1]$
$[x]$	$[0]$	$[x]$	$[x+1]$	$[1]$
$[x+1]$	$[0]$	$[x+1]$	$[1]$	$[x]$

Из этих таблиц видно, что факторкольцо $\mathbf{F_2}[x]/(f)$ является полем (это следует также из неприводимости многочлена $f(x)=x^2+x+1$ над полем $\mathbf{F_2}$ на основании **теоремы 4.3**). Это наш первый пример конечного поля, число элементов которого не является простым чис-

лом.

3) Пусть $f(x)=x^2+2\in \mathbf{F_3}[x]$. Тогда факторкольцо $\mathbf{F_3}[x]/(f)$ состоит из $p^n=3^2$ классов вычетов $[0],[1],[2],[x],[x+1],[x+2],[2x],[2x+1],[2x+2]$. Таблицы операций факторкольца $\mathbf{F_3}[x]/(f)$ опять можно получить, производя соответствующие операции над определяющими классы вычетов многочленами с последующим приведением по модулю f. Поскольку $\mathbf{F_3}[x]/(f)$ - коммутативное кольцо, достаточно найти лишь элементы таблиц операций, стоящие на главной диагонали и над нею.

+	$[0]$	$[1]$	$[2]$	$[x]$	$[x+1]$	$[x+2]$	$[2x]$	$[2x+1]$	$[2x+2]$
$[0]$	$[0]$	$[1]$	$[2]$	$[x]$	$[x+1]$	$[x+2]$	$[2x]$	$[2x+1]$	$[2x+2]$
$[1]$		$[2]$	$[0]$	$[x+1]$	$[x+2]$	$[x]$	$[2x+1]$	$[2x+2]$	$[2x]$
$[2]$			$[1]$	$[x+2]$	$[x]$	$[x+1]$	$[2x+2]$	$[2x]$	$[2x+1]$
$[x]$				$[2x]$	$[2x+1]$	$[2x+2]$	$[0]$	$[1]$	$[2]$
$[x+1]$					$[2x+2]$	$[2x]$	$[1]$	$[2]$	$[0]$
$[x+2]$						$[2x+1]$	$[2]$	$[0]$	$[1]$
$[2x]$							$[x]$	$[x+1]$	$[x+2]$
$[2x+1]$								$[x+2]$	$[x]$
$[2x+2]$									$[x+1]$

·	[0]	[1]	[2]	[x]	[x+1]	[x+2]	[2x]	[2x+1]	[2x+2]
[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]		[1]	[2]	[x]	[x+1]	[x+2]	[2x]	[2x+1]	[2x+2]
[2]			[1]	[2x]	[2x+2]	[2x+1]	[x]	[x+2]	[x+1]
[x]				[1]	[x+1]	[2x+1]	[2]	[x+2]	[2x+2]
[x+1]					[2x+2]	[0]	[2x+2]	[0]	[x+1]
[x+2]						[x+2]	[x+2]	[2x+1]	[0]
[2x]							[1]	[2x+1]	[x+1]
[2x+1]								[x+2]	[0]
[2x+2]									[2x+2]

Заметим, что факторкольцо $\mathbf{F}_3[x]/(f)$ не является полем (и даже не является целостным кольцом). Это соответствует и теореме 4.3, поскольку $f(x)=x^2+2=(x+1)(x+2)$ приводим над $\mathbf{F}_3$.

Порядок многочлена и примитивный многочлен

У каждого ненулевого многочлена f над конечным полем кроме его сте-

пени deg(f) имеется еще одна важная целочисленная характеристика - его порядок [2].

Определение: Пусть $f(x)\in \mathbf{F_q}[x]$ - ненулевой многочлен. Если $f(0)\neq 0$, то наименьшее натуральное число e, для которого многочлен $f(x)$ делит x^e-1, называется ***порядком*** многочлена $f(x)$ и обозначается $\mathrm{ord}(f)=\mathrm{ord}(f(x))$. Если же $f(0)=0$, то многочлен $f(x)$ однозначно представим в виде $f(x)=x^h g(x)$, где $h\in \mathbf{N}$, $g\in \mathbf{F_q}[x]$ и $g(0)\neq 0$, и в этом случае порядок $\mathrm{ord}(f)$ многочлена f определяется как $\mathrm{ord}(g)$.

Следствие

Если $f(x)\in \mathbf{F_q}[x]$ - неприводимый многочлен степени m над полем $\mathbf{F_q}$, то его порядок делит число q^m-1.

На основании доказанного можно дать следующую общую формулу для порядка многочлена. При этом предполагается, что все рассматриваемые многочлены имеют положительную степень и ненулевой постоянный член.

Теорема

Пусть $\mathbf{F_q}$ — конечное поле характеристики p. Если $f = af_1^{n_1}\ldots f_k^{n_k}$ - каноническое разложение в кольце $\mathbf{F_q}[x]$ многочлена $f(x)\in \mathbf{F_q}[x]$ положительной степени, такого, что $f(0)\neq 0$ (т.е. $a\in \mathbf{F_q}$, $n_1,\ldots,n_k\in \mathbf{N}$ и $f_1,\ldots,f_k$ - различные нормированные неприводимые многочлены из $\mathbf{F_q}[x]$, отличные от x), то

$$\mathrm{ord}\,(f) = \mathrm{ord}(af_1^{n_1}\ldots f_k^{n_k})=p^t\mathrm{НОК}(\mathrm{ord}\,(f_1),\ldots,\mathrm{ord}(f_k)),$$

где t - наименьшее целое число, удовлетворяющее неравенству $p^t \geq \max(n_1,\ldots,n_k)$.

Определение: Многочлен $f(x)\in \mathbf{F_q}[x]$ степени m является ***примитивным***

многочленом над $\mathbf{F_q}$ в том и только том случае, если он - нормированный многочлен, такой, что $f(0)\neq 0$ и $\mathrm{ord}(f)=q^m-1$.

Данное определение является формулировкой теоремы. Реальное определение примитивного многочлена потребовало бы от нас введения некоторого дополнительного понятия, в пределах же данного курса можно ограничиться последним.

Задания

3.4.1 Вычислить остаток и частное от деления многочленов

$f(x)=x^6+x^5+x^4+x^2+1$ на $g(x)=x^3+x+1$ над $\mathbf{F}_2$

$q(x)=x^3+x^2$ $r(x)=1$

$f(x)=x^8+x^7+x^4+x^3+1$ на $g(x)= x^5+x^3+x^2+1$ над $\mathbf{F}_2$

$q(x)=x^3+x^2+x$ $r(x)=x^4+x^3+x^2+x+1$

3.4.2 Вычислить НОД($f(x)$,$g(x)$)

$f(x)=x^5+x^3+2x^2+1$ на $g(x)=x^3+2x+1$ над $\mathbf{F_5}$ 1

$f(x)= x^6+ 3x^5+2x^4+4x^3+4x^2+3x$ на $g(x)=x^3+3x^2+2x+3$ над $\mathbf{F_5}$ 1

$f(x)=x^6+x^4+x+1$ на $g(x)=x^3+x+1$ над $\mathbf{F_2}$ x^3+x+1

$f(x)=x^6+2x^3+x^2+1$ на $g(x)=x^5+2x^4+1$ над $\mathbf{F_3}$ 1

3.4.3 Проверить многочлен на неприводимость

$f(x)=x^6+x^3+1$ неприводим

$f(x)=x^6+x^4+x+1$ приводим

$f(x)=x^6+x^5+x^4+1$ приводим

3.4.4 Вычислить порядок многочлена

$f(x)=x^3+1$ над $\mathbf{F_2}$ 3

$f(x)=x^4+x^2+x+1$ над $\mathbf{F_2}$ 7

$f(x)=x^5+x+1$ над $\mathbf{F_2}$ 21

$f(x)= x^6+ x^4+x^2+x+1$ над $\mathbf{F_2}$ *21*

§IV.5. РЕГИСТРЫ СДВИГА С ОБРАТНОЙ СВЯЗЬЮ. СВОЙСТВА ПЕРИОДИЧНОСТИ

Пусть k — натуральное число, а a, a_0, a_1 ..., a_{k-1} — заданные элементы конечного поля $\mathbf{F_q}$. Последовательность s_0, s_1.,... элементов поля $\mathbf{F_q}$, удовлетворяющая соотношению

$$s_{n+k} = a_{k-1}s_{n+k-1}+a_{k-2}s_{n+k-2}+\ldots+a_0s_n+a, \quad n = 0,\ 1,\ldots \quad (5.1)$$

называется ***линейной рекуррентной последовательностью k-го порядка*** над полем $\mathbf{F_q}$. Первые члены s_0, s_1 ..., s_{k-1} однозначно определяют всю последовательность и называются ее ***начальными значениями***. Линейное рекуррентное соотношение называется ***однородным***, если $a=0$, в противном случае линейное рекуррентное соотношение будет называться ***неоднородным***. Соответствующая рекуррентная последовательность s_0, s_1 ... будет называться ***однородной*** (или ***неоднородной***) ***линейной рекуррентной последовательностью*** над полем $\mathbf{F_q}$.

Однородную линейную рекуррентную последовательность модно задать соотношением

$$s_{n+k} = a_{k-1}s_{n+k-1}+a_{k-2}s_{n+k-2}+\ldots+a_0s_n, \quad n = 0,\ 1,\ldots \quad (5.2)$$

Линейные рекуррентные последовательности можно получать с помощью ***регистров сдвига с обратной связью***. Пример регистра сдвига с обратной связью изображен на рисунке 5.1.

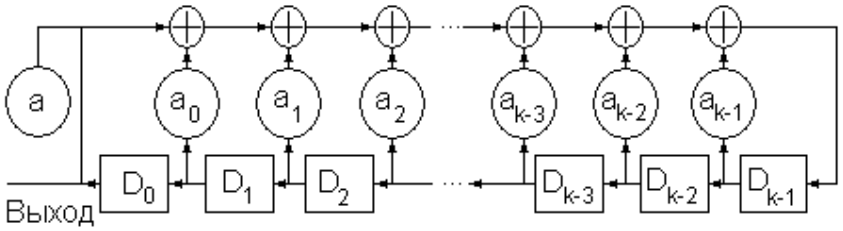


Рисунок 5.1 – Регистр сдвига с линейной обратной связью.

Поясним вид и назначение элементов регистров сдвига [2].

Сумматор имеет два входа и один выход. Если на входе появляются два элемента поля $\mathbf{F_q}$, то выходом является их сумма в поле $\mathbf{F_q}$.

Усилитель имеет один вход и один выход. Если на вход поступает элемент поля $\mathbf{F_q}$, то на выходе усилителя появляется его произведение на некоторый постоянный элемент из поля $\mathbf{F_q}$.

Увеличитель работает аналогично усилителю, но в отличие от него прибавляет к поступающему на вход элементу некоторый элемент поля $\mathbf{F_q}$.

***Элемент задержки* (*триггер*)** - имеет один вход и один выход, его работа регулируется внешним синхронизирующим частотным генератором, таким образом, что элемент поля $\mathbf{F_q}$, поступивший на вход в данный момент времени, появляется в качестве выхода в следующий момент времени (т.е. на следующем такте работы).

Сумматор

Усилитель (умножает на элемент *a*)

Увеличитель (прибавляет элемент *a*)

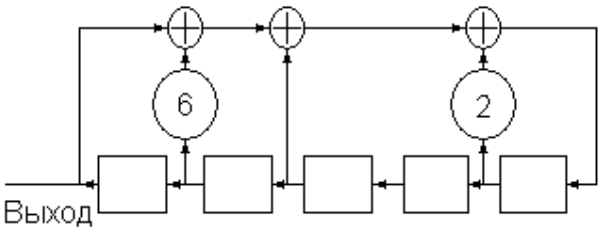
Элемент (триггер)

Рисунок 5.2

В начале работы каждый элемент задержки D_i, $i = 0, 1, \ldots k - 1$, содержит некоторое начальное заполнение s_i. Если считать, что выполнение арифметических операций и передача сигналов по проводам происходят мгновенно, то на следующем такте работы каждый элемент задержки D_i содержит заполнение s_{i+1}. Продолжая этот процесс, мы видим, что выходом регистра сдвига с обратной связью является последовательность элементов s_0, s_1, s_2, …, получаемых в последовательные моменты времени. Для большинства приложений используются однородные линейные рекуррентные последовательности, в этом случае увеличитель в конструкции соответствующего регистра сдвига не требуется.

Пример 1

Построим в поле $\mathbf{F_7}$ регистр сдвига с линейной обратной связью (РСЛОС) в соответствии с однородным линейным рекуррентным соотношением $s_{n+5} = 2s_{n+4} + s_{n+2} + 6s_{n+1} + s_n$.

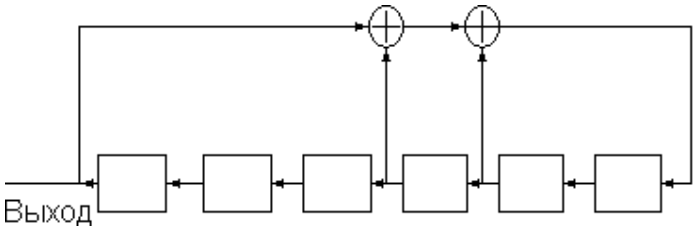


Поскольку a_{n+3} равен 0, соответствующий сумматор отсутствует.

Пример 2

Построим в поле $\mathbf{F_2}$ регистр сдвига с линейной обратной связью в

соответствии с однородным линейным рекуррентным соотношением $s_{n+6} = s_{n+4} + s_{n+3} + s_n$. Поскольку мы работаем в поле $\mathbf{F_2}$, у нас отпадает надобность использовать усилители, сигнал без усиления поступает на сумматоры. РСЛОС будет выглядеть следующим образом.



Проследим динамику линейной рекуррентной последовательности.

	S_n	S_{n+1}	S_{n+2}	S_{n+3}	S_{n+4}	S_{n+5}
0	*1*	*0*	*0*	*0*	*0*	*0*
1	*0*	*0*	*0*	*0*	*0*	*1*
2	*0*	*0*	*0*	*0*	*1*	*0*
3	*0*	*0*	*0*	*1*	*0*	*1*
4	*0*	*0*	*1*	*0*	*1*	*1*
5	*0*	*1*	*0*	*1*	*1*	*1*
6	*1*	*0*	*1*	*1*	*1*	*0*
7	*0*	*1*	*1*	*1*	*0*	*1*
8	*1*	*1*	*1*	*0*	*1*	*1*
9	*1*	*1*	*0*	*1*	*1*	*0*
10	*1*	*0*	*1*	*1*	*0*	*1*
11	*0*	*1*	*1*	*0*	*1*	*0*
12	*1*	*1*	*0*	*1*	*0*	*1*
13	*1*	*0*	*1*	*0*	*1*	*0*
14	*0*	*1*	*0*	*1*	*0*	*0*
15	*1*	*0*	*1*	*0*	*0*	*1*
16	*0*	*1*	*0*	*0*	*1*	*1*
17	*1*	*0*	*0*	*1*	*1*	*1*
18	*0*	*0*	*1*	*1*	*1*	*1*
19	*0*	*1*	*1*	*1*	*1*	*0*
20	*1*	*1*	*1*	*1*	*0*	*0*
21	*1*	*1*	*1*	*0*	*0*	*0*
22	*1*	*1*	*0*	*0*	*0*	*1*
23	*1*	*0*	*0*	*0*	*1*	*1*

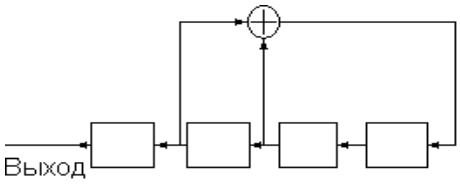
24	*0*	*0*	*0*	*1*	*1*	*0*
25	*0*	*0*	*1*	*1*	*0*	*0*
26	*0*	*1*	*1*	*0*	*0*	*1*
27	*1*	*1*	*0*	*0*	*1*	*0*
28	*1*	*0*	*0*	*1*	*0*	*0*
29	*0*	*0*	*1*	*0*	*0*	*0*
30	*0*	*1*	*0*	*0*	*0*	*0*
31	*1*	*0*	*0*	*0*	*0*	*0*
32	*0*	*0*	*0*	*0*	*0*	*1*
33	*0*	*0*	*0*	*0*	*1*	*0*

Продолжать таблицу не имеет смысла, поскольку уже на *31*-м столбце очевидна периодичность нашей последовательности. Наша последовательность имеет период в *31* шаг.

Пример 3

Приведем еще один показательный пример.

Построим в поле $\mathbf{F_2}$ регистр сдвига с линейной обратной связью в соответствии с однородным линейным рекуррентным соотношением $s_{n+4} = s_{n+2} + s_{n+1}$ и проследим его динамику.



	S_n	S_{n+1}	S_{n+2}	S_{n+3}
0	*1*	*1*	*0*	*1*
1	*1*	*0*	*1*	*1*
2	*0*	*1*	*1*	*1*
3	*1*	*1*	*1*	*0*
4	*1*	*1*	*0*	*0*
5	*1*	*0*	*0*	*1*
6	*0*	*0*	*1*	*0*
7	*0*	*1*	*0*	*1*
8	*1*	*0*	*1*	*1*
9	*0*	*1*	*1*	*1*
10	*1*	*1*	*1*	*0*

Периодичность нашей последовательности проявилась с *1*-го по *7* шаг, однако начальное заполнение более не встречалось. В дальнейшем, подобную не периодичную последовательность будем называть ***предпериодом***, и оговорим когда он встречается.

Любая линейная рекуррентная последовательность периодична, после некоторого предпериода (а возможно и без) проявляются ее периодические свойства.

Пусть s_0, s_1,... – линейная рекуррентная последовательности *k*-го порядка над полем $\mathbf{F_q}$, удовлетворяющая соотношение (5.1). Как уже было отмечено, эту последовательность можно получить с помощью регистра сдвига с обратной связью, изображенного на рис. 5.1. Если *n* — целое неотрицательное число, то через *n* тактов работы элемент задержки D_j, $j = 0,1, \ldots, k-1$, будет

содержать заполнение s_{n+j}. Таким образом, вектор $s_n = (s_n, s_{n+1}, \ldots s_{n+k-1})$ естественно назвать ***вектором n-го состояния*** линейной рекуррентной последовательности (или ***внутренним состоянием*** регистра сдвига с обратной связью ***на n-м такте*** работы). Вектор состояния $s_0 = (s_0, s_1, \ldots, s_{k-1})$ называется ***вектором начального состояния***.

Определение: Пусть **S** – произвольное непустое множество, и пусть s_0, s_1, ... – последовательность элементов из множества **S**, Если существуют целые числа $r > 0$ и $n_0 > 0$, такие, что $s_{n+r} = s_n$ для всех $n > n_0$, то последовательность s_0, s_1, ... называется ***периодической последовательностью***, а r — ***периодом*** указанной последовательности. Наименьший из всех возможных периодов периодической последовательности называется ***минимальным периодом*** последовательности.

Лемма 5.1

Каждый период периодической последовательности делится на ее минимальный период.

Доказательство

Пусть r — произвольный период периодической последовательности s_0, s_1 ..., и пусть ρ - ее минимальный период. Из этого следует, что $s_{n+r} = s_n$ для всех $n \geq n_0$, а $s_{n+\rho} = s_n$ для всех $n > n_1$ при соответствующем выборе n_0 и n_1. Если r не делится на ρ, то, применяя теорему деления целых чисел, представим r в виде $r = m\rho + t$, где $m > 1$ и $0 < t < \rho$. Тогда для всех $n \geq max\,(n_0, n_1)$ получаем

$$s_n = s_{n+r} = s_{n+m\rho+t} = s_{n+(m-1)\rho+t} = \ldots = s_{n+t},$$

откуда следует, что t (которое меньше ρ) также является периодом последовательности s_0, s_1, ... Это противоречит тому, что ρ — минимальный период последовательности. ■

Определение: Периодическая последовательность s_0, s_1, ... с минимальным периодом r называется ***чисто периодической***, если равенство $s_{n+r} = s_n$

выполняется для всех $n = 0, 1, \ldots$.

Пусть s_0, s_1 ... — периодическая последовательность, а r — ее минимальный период. Наименьшее неотрицательное целое число n_0, такое, что $s_{n+r} = s_n$ для всех $n \geq n_0$, называется ***предпериодом*** этой последовательности. Периодическая последовательность является чисто периодической, если ее предпериод равен 0.

Теорема 5.2

Пусть $\mathbf{F_q}$ – произвольное конечное поле, а k - некоторое натуральное число. Тогда каждая линейная рекуррентная последовательность k-го порядка над полем $\mathbf{F_q}$ является периодической. При этом ее минимальный период r удовлетворяет неравенству $r \leq q^k$, а в случае однородной последовательности – равенству $r \leq q^k - 1$.

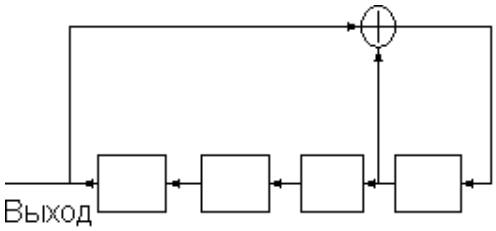
Пояснение

Всего существует q^k Различных упорядоченных наборов по k элементов из поля $\mathbf{F_q}$.Это значит, что максимальный период ЛРП k-го порядка равен q^k, однако если однородное линейное рекуррентное соотношение заполнить нулевым вектором начального состояния, то каждый последующий вектор состояния будет так же нулевым. Поэтому при однородном линейном рекуррентном соотношении нулевой вектор состояния не может появиться, получаем, что $r \leq q^k–1$. Если же рекуррентное соотношение будет неоднородным, то даже при нулевом векторе начального состояния следующий вектор состояния будет не нулевым и в этом случае $r \leq q^k$.

Пример4

Ситуацию когда $r < q^k–1$, мы наблюдали на предыдущих примерах, приведем пример когда $r = q^k–1$. Построим РСЛОС в соответствии с линейным рекуррентным соотношением $s_{n+4} = s_{n+3} + s_n$ и проследим его динамику.

РСЛОС отвечающий заданному соотношению имеет следующий вид.



	S_n	S_{n+1}	S_{n+2}	S_{n+3}
0	*1*	*1*	*0*	*1*
1	*1*	*0*	*1*	*0*
2	*0*	*1*	*0*	*1*
3	*1*	*0*	*1*	*1*
5	*0*	*1*	*1*	*0*
6	*1*	*1*	*0*	*0*
7	*1*	*0*	*0*	*1*
8	*0*	*0*	*1*	*0*
9	*0*	*1*	*0*	*0*
10	*1*	*0*	*0*	*0*
11	*0*	*0*	*0*	*1*
12	*0*	*0*	*1*	*1*
13	*0*	*1*	*1*	*1*
14	*1*	*1*	*1*	*1*
15	*1*	*1*	*1*	*0*
16	*1*	*1*	*0*	*1*
17	*1*	*0*	*1*	*0*

Очевидно, что период данной рекуррентной последовательности ра-

вен $r = q^k - 1 = \quad = 2^4 - 1 = 15$. Максимальный период. Теперь заполним вектор начального состояния нулевыми значениями.

	S_n	S_{n+1}	S_{n+2}	S_{n+3}
0	*0*	*0*	*0*	*0*
1	*0*	*0*	*0*	*0*
2	*0*	*0*	*0*	*0*

Теорема 5.3

Пусть s_0, s_1 ... — линейная рекуррентная последовательность над конечным полем, удовлетворяющая линейному рекуррентному соотношению (5.1). Если коэффициент a_0 в (5.1) не равен *0*, то последовательность s_0, s_1 ... является чисто периодической.

Доказательство

Пусть r — минимальный период ЛРП s_0, s_1 ..., а n_0 — предпериод, тогда $s_{n+r} = s_n$ для всех $n \geq n_0$. Допустим, что в нашем случае $n_0 \geq 1$. Из соотношения (5.1)

$s_{n+k} = a_{k-1}s_{n+k-1} + a_{k-2}s_{n+k-2} + ... + a_0 s_n + a$, полагая $n = n_0 + r - 1$ получим

$s_{n_0+r-1+k} = a_{k-1}s_{n_0+r+k-2} + a_{k-2}s_{n_0+r+k-3} + ... + a_0 s_{n_0+r-1} + a$, выразим из этого выражения $a_0 s_{n_0+r-1}$

$a_0 s_{n_0+r-1} = s_{n_0+r-1+k} - a_{k-1}s_{n_0+r+k-2} - a_{k-2}s_{n_0+r+k-3} - ... - a_1 s_{n_0-r} - a$,

поскольку последовательность периодична, можем избавиться от r

$a_0 s_{n_0+r-1} = s_{n_0+1+k} - a_{k-1}s_{n_0+k-2} - a_{k-2}s_{n_0+k-3} - ... - a_1 s_{n_0} - a$, т.к $a_0 \neq 0$, можем для него найти обратное, получаем

$s_{n_0+r-1} = a_0^{-1}(s_{n_0+1+k} - a_{k-1}s_{n_0+k-2} - a_{k-2}s_{n_0+k-3} - ... - a_1 s_{n_0} - a)$

Теперь воспользовавшись соотношением (5.1) для $n = n_0 - 1$, приходим к такому же выражению и для s_{n_0-1}, откуда следует равенство $s_{n_0-1} = s_{n_0+r-1}$. Последнее противоречит тому, что n_0 является предпериодом последовательно-

сти s_0, s_1 ….■

Из всех однородных линейных рекуррентных последовательностей над полем $\mathbf{F_q}$, удовлетворяющих данному линейному рекуррентному соотношению k-го порядка вида (5.2), можно выделить одну последовательность с максимальным значением минимального периода, называемую ***импульсной функцией*** или ***последовательностью, порожденной импульсом*** [2]. Эта последовательность обозначается d_0, d_1 ... и однозначно определяется начальными значениями $d_0 = ... = d_{k-2}=0$, $d_{k-1} = 1$ ($d_0 = 1$ для $k = 1$) и линейным рекуррентным соотношением

$$d_{n+k} = a_{k-1}d_{n+k-1}+a_{k-2}d_{n+k-2}+\ldots+a_0d_n, \quad n = 0, 1,... \qquad (5.3)$$

Теорема 5.4

Минимальный период однородной линейной рекуррентной последовательности над полем $\mathbf{F_q}$ делит минимальный период соответствующей импульсной функции.

Пример 5

Построим линейную рекуррентную последовательность над полем F_2 заданную соотношением $s_{n+5} = s_{n+4} + s_{n+3} + s_n$, и определим период, с начальным заполнением – импульсной функцией (*0 0 0 0 1*), а так же с начальным заполнением следующего вида (*1 0 0 1 1*).

0 0 0 0 1 1 0 1 1 1 1 0 0 1 0 0 0 0 1…

Поскольку $a_0 \neq 0$ предпериод отсутствует. Период последовательности равен *14*.

Пять любых последовательных элементов взятых из данной последовательности в качестве вектора начального состояния дадут последовательность того же периода.

1 0 0 1 1 1 0 1 0 0 1 1 1 0 1 0 0 1 1 …

1 0 1 1 0 0 0 1 0 1 1 0 0 0 1 0 1 1 0 …

Период данных последовательностей равен *7*.

1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 …

0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 …

Период данных последовательностей равен *1*.

1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 …

Период последовательности равен *2*.

Мы перечислили всевозможные последовательности, порождаемые соотношением $s_{n+5} = s_{n+4} + s_{n+3} + s_n$. На данном примере мы можем убедиться в справедливости теоремы*5.4*. Максимальный период данного рекуррентного соотношения, при начальном заполнении *0 0 0 0 1*, равен *14*(импульсная функция). При заполнении *1 0 0 1 1* и *1 0 1 1 0* – период равен *7*, при *0 1 0 1 0* – период *2* и при *1 1 1 1 1* и *0 0 0 0 0* период равен *1*. Минимальный период любой из последовательностей соотношения $s_{n+5} = s_{n+4} + s_{n+3} + s_n$ делит минимальный период импульсной функции.

Пусть $s_0, s_1,...$ — линейная однородная рекуррентная последовательность k-го порядка над полем $\mathbf{F_q}$, удовлетворяющая линейному рекуррентному соотношению

$$s_{n+k} = a_{k-1}s_{n+k-1} + a_{k-2}s_{n+k-2} + \ldots + a_0 s_n,\ n = 0, 1, \ldots, \quad (5.4)$$

где a_j принадлежит $\mathbf{F_q}$, $0 \le j \le k-1$. Многочлен

$$f(x) = x^k - a_{k-1}x^{k-1} - a_{k-2}x^{k-2} - \ldots - a_0$$

принадлежащий $\mathbf{F_q}[x]$ называется ***характеристическим многочленом*** данной линейной рекуррентной последовательности. Он зависит только от линейного рекуррентного соотношения (5.4).

Теорема 5.5

Пусть s_0, s_1,... - однородная линейная рекуррентная последовательность над полем $\mathbf{F_q}$ и $f(x)\in\mathbf{F_q}[x]$ характеристический многочлен этой последовательности. Тогда минимальный период этой последовательности делит ord($f(x)$), а минимальный период соответствующей импульсной функции равняется ord($f(x)$). При этом если $f(0)\neq 0$, то обе последовательности являются чисто периодическими.

Теорема 5.6

Пусть $s_0,s_1,...$- однородная линейная рекуррентная последовательность над полем $\mathbf{F_q}$ с ненулевым вектором начального состояния. Пусть ее характеристический многочлен $f(x)\in\mathbf{F_q}[x]$ является неприводимым многочленом над полем $\mathbf{F_q}$, и удовлетворяет условию $f(0)\neq 0$. Тогда последовательность $s_0,s_1,...$ является чисто периодической последовательностью и ее минимальный период r равен ord($f(x)$).

Теорема 5.7

Пусть $f(x)\in\mathbf{F_q}[x]$ - неприводимый многочлен над полем $\mathbf{F_q}$ и deg($f(x)$)=k. Тогда ord($f(x)$) делит q^k-1.

Пример 6

Рассмотрим линейное рекуррентное соотношение $s_{n+6}=s_{n+4}+s_{n+2}+s_{n+1}+s_n$, $n=0, 1,...$, над полем $\mathbf{F_2}$. Соответствующий характеристический многочлен

$f(x)=x^6+x^4 - x^2-x-1\in\mathbf{F_q}[x]$ является неприводимым многочленом над полем $\mathbf{F_2}$,. Кроме того, $f(x)$ делит $x^{21}-1$ и не является делителем многочлена вида x^e-1 ни для какого $0<e<21$. Таким образом, ord($f(x)$)=21. Импульсная функция, соответствующая данному рекуррентному соотношению, имеет вид

0,0,0,0,0,1,0,1,0,0,1,0,0,1,1,0,0,1,0,1,1,0,0,0,0,0,1,....

Как и должно быть, эта последовательность периодична с минимальным периодом $r=21$. Если в качестве вектора начального состояния взять вектор $(0,0,0,0,1,1)$, то мы получим бинарную последовательность

$0,0,0,0,1,1,1,1,0,1,1,0,1,0,1,0,1,1,1,0,1,0,0,0,0,1,1\ldots$

с минимальным периодом $r=21$. Если же в качестве вектора начального состояния взять вектор $(0,0,0,1,0,0)$, то мы получим бинарную последовательность

$0,0,0,1,0,0,0,1,1,0,1,1,1,1,1,1,0,0,1,1,1,0,0,0,1,0,0,...$

также имеющую минимальный период 21. При этом каждый из ненулевых 6-мерных векторов над полем F_2 появляется в качестве вектора состояния в точности в одной из этих трех последовательностей. Если в качестве вектора начального состояния взять любой ненулевой вектор, то мы получим рекуррентную последовательность, имеющую минимальный период, равный 21, и совпадающую с точностью до сдвига с одной из трех полученных выше последовательностей.

Пример 7

Если многочлен $f(x)\in \mathbf{F_q}[x]$ степени k приводим, то его порядок $\mathrm{ord}(f(x))$ не обязательно делит число q^k-1. Чтобы показать это, рассмотрим, например, многочлен $f(x)=x^5+x+1\in \mathbf{F_2}[x]$. Этот многочлен приводим, так как

$f(x)=x^5+x+1=(x^3+x^2+1)\cdot(x^2+x+1)$.

Для приложений особый интерес представляют линейные рекуррентные последовательности, имеющие очень большой минимальный период. Из **теоремы 5.2** известно, что для однородной линейной рекуррентной последовательности k-го порядка над полем $\mathbf{F_q}$ минимальный период не может превы-

шать q^k-*1*. Для того чтобы построить рекуррентную последовательность, минимальный период которой в точности равен q^k-*1*, воспользуемся понятием примитивного многочлена [2].

Определение: Однородная линейная рекуррентная последовательность над полем $\mathbf{F_q}$, характеристический многочлен которой является примитивным многочленом над полем $\mathbf{F_q}$, а вектор начального состояния - ненулевым вектором, называется последовательностью максимального периода над полем $\mathbf{F_q}$.

Теорема 5.8

Каждая последовательность *k*-го порядка и максимального периода над полем $\mathbf{F_q}$ является чисто периодической последовательностью, а ее минимальный период равняется q^k-*1*, наибольшему из возможных значений, которое может принимать минимальный период однородной линейной рекуррентной последовательности *k*-го порядка над полем $\mathbf{F_q}$.

Задания

3.5.1 Построить РСЛОС для следующих ЛРП

$s_7=s_5+s_3+s_2+s_0$

$s_9=s_7+s_5+s_2+s_0$

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Виноградов И.М. Основы теории чисел. - 10-е изд., стер. - СПб.: Издательст-во "Лань", 2004. - 176 с. - (Учебники для вузов. Специальная литература).

2. Лидл Р. Нидерайтер Г. Конечные поля. В 2-х т. Т.1. Пер. с англ. - М.:Мир, 1988. -430 с.

3. Сизый С. В. Лекции по теории чисел (Учебное пособие для математических специальностей) - Екатеринбург: Уральский государственный университет им. А.М.Горького, 1999.

4. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. - М.:МЦНМО, 2003.-328 с.

5. Саломаа А. Криптография с открытым ключом. - Пер. с англ. - М.: Мир, 1995. - 318 с., ил.

6. Черемушкин А.В. Лекции по арифметическим алгоритмам в криптографии. - М. МЦНМО, 2002. -104 с.

7. Кнут Д.Э. Искусство программирования. - 1-е издание, М.:Мир, 1977.

8. Аркитас А. Основы компьютерной алгебры с приложениями. Пер. с англ. - М.:Мир, 1994. - 544 с., ил.

9. Прокл Диадох. Комментарий к первой книге "Начал" Евклида.

10. Евклид и его «Начала». Сайт: http://www.bolshe.ru/book/id=2487

11. Энциклопедический словарь юного математика, 2-е издание, 1989г.

12. Тим Р. Леонард Эйлер. Киев, 1983.

13. Постников М. М. "Теорема Ферма", М., 1978

14. Поточные шифры, результаты зарубежной криптографии.

15. W.H.Press, B.P.Flannery, S.A. Teukolsky and W.T. Vetterling, *Numerical*

Recipes in C: The Art of Scientific Computing, Cambridge University Press, 1988.

16. J. Plumstead (Boyar). Inferring a sequence generated by a linear congruence. In Proceedings of 23rd IEEE Symposium on Foundations of Computer Science, pages 153-159, 1982.

17. Фомичёв В.М. Дискретная математика и криптология (курс лекций). - М.:ДИАЛОГ-МИФИ, 2003. – 400 с.

18. Баричев С.Г. Серов Р.Е. Основы современной криптографии, электронное издание, 2003. -152 с.

19. Эвриаст Галуа. Сайт: http://mathem.by.ru/galua.html