Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

Кафедра интеллектуальных информационных технологий

Ю. В. Виланский, В. В. Захаров

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Лабораторный практикум
для студентов специальности «Искусственный интеллект»
всех форм обучения

В 2-х частях

Часть 1

Минск БГУИР 2010

УДК 621.391.25(076.5)
ББК 32.811я73
В44

Р е ц е н з е н т

заведующий кафедрой автоматизированных систем управления войсками учреждения образования «Военная академия Республики Беларусь», кандидат технических наук, доцент А. В. Хижняк

Виланский, Ю. В.

В44 Криптографические методы защиты информации : лаб. практикум для студ. спец. «Искусственный интеллект» всех форм обуч. В 2 ч. Ч. 1 / Ю. В. Виланский, В. В. Захаров. – Минск : БГУИР, 2010. – 40 с. : ил.

ISBN 978-985-488-525-4 (ч. 1).

Содержит теоретические сведения, упражнения для самостоятельной работы и задания для выполнения лабораторных работ по дисциплине «Криптографические методы защиты информации».

Предназначен для студентов специальности «Искусственный интеллект» по специализации «Интеллектуальные компьютерные технологии защиты информации».

УДК 621.391.25(076.5)
ББК 32.811я73

ISBN 978-9855-488-525-4 (ч. 1)
ISBN 978-9855-488-524-7

Содержание

ВВЕДЕНИЕ

Криптографические методы широко применяются в современных компьютерных системах, без их использования невозможно создать надежные механизмы защиты, обеспечивающие такие фундаментальные функции безопасности, как конфиденциальность, целостность, аутентификация, подтверждение авторства.

В настоящее время разработано большое количество разнообразных криптографических алгоритмов и протоколов. Эти алгоритмы и протоколы различаются сферой применения, требованиями к ресурсам и производительности вычислительных систем, показателями стойкости и т. д. Перед разработчиками систем защиты в нынешних условиях редко стоит задача разработки нового криптографического алгоритма или протокола. Законодательство многих стран содержит требования, ограничивающие применения методов шифрования или электронной цифровой подписи конкретными алгоритмами. Однако существенной особенностью практически любых всех криптографических алгоритмов является необходимость их правильного встраивания в реальные механизмы защиты. Можно привести большое количество примеров, когда даже очень стойкие и надежные криптографические алгоритмы оказывались неэффективными из-за неправильного применения.

Целью данного лабораторного практикума является формирование у студентов навыков правильного внедрения криптографических средств, для получения которых необходимо понять особенности математических моделей, лежащих в основе конкретных алгоритмов и протоколов.

ЛАБОРАТОРНАЯ РАБОТА №1
АНАЛИЗ И ГЕНЕРАЦИЯ СЛУЧАЙНЫХ И ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Теоретические сведения

Современная информатика широко использует псевдослучайные числа в самых разных приложениях – от метода Монте-Карло и имитационного моделирования до криптографии. При этом от качества используемых ГПСЧ напрямую зависит качество получаемых результатов.

В теории вероятностей случайная величина имеет **дискретное равномерное распределение**, если она принимает конечное число значений с равными вероятностями.

Никакой детерминированный алгоритм не может генерировать полностью случайные числа, а только лишь аппроксимировать некоторые свойства случайных чисел.

Любой ГПСЧ с ограниченными ресурсами рано или поздно зацикливается. Длина циклов ГПСЧ зависит от самого генератора и в среднем составляет около $2^{n/2}$, где n – это размер внутреннего состояния в битах. Если ГПСЧ может сходиться к слишком коротким циклам, такой ГПСЧ становится предсказуемым и является непригодным.

Большинство простых арифметических генераторов, хотя и обладают большой скоростью, но страдают от многих серьезных недостатков:

- слишком короткий период/периоды;
- последовательные значения не являются независимыми;
- некоторые биты «менее случайны», чем другие;
- неравномерное одномерное распределение;
- обратимость.

В качестве примеров эффективно реализуемых на компьютерах алгоритмов генерации случайных последовательностей можно привести четыре генератора с периодом $T_{\max} \approx 2^{96}$ (1.1 – 1.4):

$$x_n = (1176x_{n-1} + 1476x_{n-2} + 1776x_{n-3}) \bmod (2^{32} - 5); \quad (1.1)$$

$$x_n = 2^{53}(x_{n-1} + x_{n-2} + x_{n-3}) \bmod (2^{32} - 5); \quad (1.2)$$

$$x_n = (1995x_{n-1} + 1998x_{n-2} + 2001x_{n-3}) \bmod (2^{32} - 849); \quad (1.3)$$

$$x_n = 2^{53}(x_{n-1} + x_{n-2} + x_{n-3}) \bmod (2^{32} - 1629). \quad (1.4)$$

Одной из особенностей использования ГПСЧ является необходимость оценки качества генерируемой последовательности. Не существует универсальных средств, позволяющих однозначно оценить «случайность» выходной последовательности ГСЧ. Самым простым из них является известный критерий хи-квадрат.

Рассмотрим **средства оценки качества последовательностей.**

Программа Expert.exe. Эта программа реализует проверку заданного фала на «случайность» в соответствии с простейшим критерием хи-квадрат для 256 степеней свободы.

Программа может анализировать любые файлы и предназначена для быстрой оценки подозрительности на случайности имеющейся последовательности. После выбора файла программа отображает гистограмму частотного распределения символов (рис. 1.1).

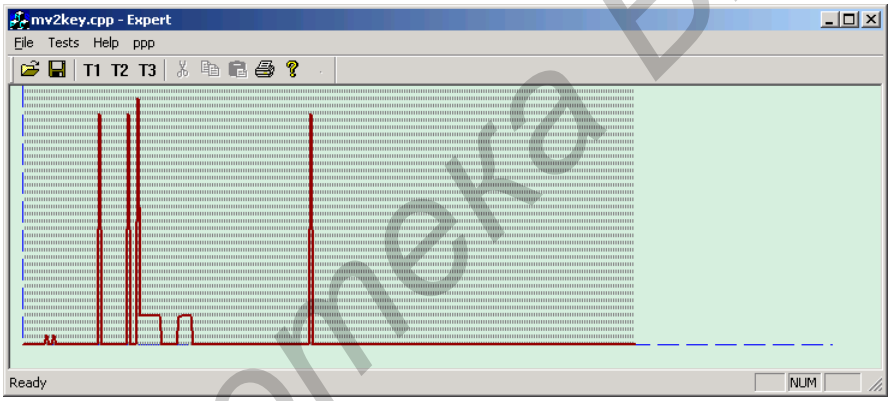

Рис. 1.1. Окно программы Expert

Для использования программы откройте файл и нажмите кнопку T1.

Программа выведет окно диалога с результатами анализа (рис. 1.2).

Программа выдает три значения:

- последовательность не является случайной;
- последовательность подозрительна;
- последовательность почти подозрительна.

Результаты «последовательность подозрительна» или «последовательность почти подозрительна» говорят о том, что выбранный файл содержит последовательность символов, похожую на случайную. В этом случае необходимо использовать более утонченные методы для оценки того, является ли сохраненная в выбранном файле последовательность достаточно случайной.

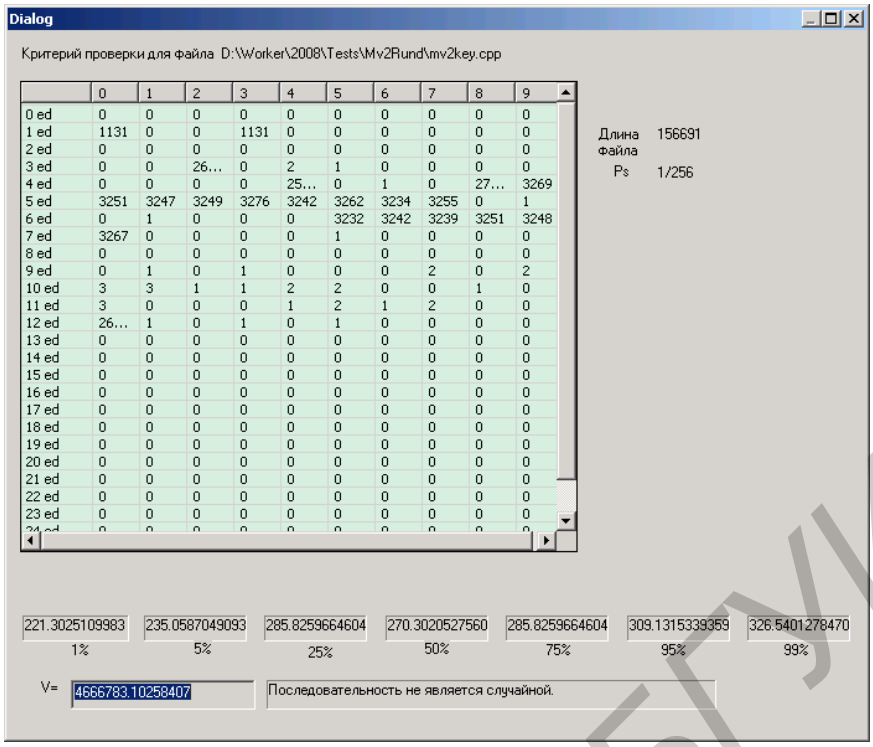

Рис. 1.2. Результат анализа на соответствии критерию хи-квадрат

Батарея тестов Диехарда. Джордж Марсалья (George Marsaglia) в течение нескольких лет разрабатывал программу, реализующую набор статистических тестов для измерения качества набора случайных чисел. Названные батарей тестов Диехарда эти тесты впервые опубликованы на CD-ROM, посвященном случайным числам. Вместе они рассматриваются как один из наиболее строгих известных наборов тестов. Батарея содержит 15 тестов, построенных на базе различных методов:

1. «Дни рождения» (Birthday Spacings). В этом тесте выбираются случайные точки на большом интервале. Расстояния между точками должны быть асимптотически распределены по Пуассону. Свое название этот тест получил на основе парадокса дней рождения.

2. «Пересекающиеся перестановки» (Overlapping Permutations) – анализируются последовательности пяти последовательных случайных чисел. 120 возможных перестановок должны получаться со статистически эквивалентной вероятностью.

3. «Ранги матриц» (Ranks of matrices) – выбирается некоторое количество бит из некоторого количества случайных чисел для формирования матрицы на {0, 1}, затем определяется ранг матрицы. Считаются ранги.

4. «Обезьяньи тесты» (Monkey Tests). В этих тестах последовательности некоторого количества бит интерпретируются как слова. Считаются пересекающиеся слова в потоке. Количество «слов», которые не появляются, должны удовлетворять известному распределению. Название этот тест получил на основе теоремы о бесконечном количестве обезьян.

5. «Подсчет единичек» (Count the 1's). Считаются единичные биты в каждом из последующих или выбранных байт. Эти счетчики преобразуется в «буквы», и считаются случаи встречи пятибуквенных «слов».

6. «Тест на парковку» (Parking Lot Test). В этом тесте единичные окружности случайно размещаются в квадрате 100×100. Если окружность пересекает уже существующую, попытаться выбрать другую окружность. После 12 000 попыток количество успешно «припаркованных» окружностей должно быть нормально распределено.

7. «Тест на минимальное расстояние» (Minimum Distance Test). 8000 точек случайно размещаются в квадрате 10 000×10 000, затем находится минимальное расстояние между любыми парами. Квадрат этого расстояния должен быть экспоненциально распределен с некоторой медианой.

8. «Тест случайных сфер» (Random Spheres Test). Случайно выбирается 4000 точек в кубе с ребром 1000. В каждой точке помещается сфера, радиус которой является минимальным расстоянием до другой точки. Минимальный объём сферы должен быть экспоненциально распределен с некоторой медианой.

9. «Тест сжатия» (The Squeeze Test). В этом тесте число 231 умножается на случайные вещественные числа в диапазоне [0, 1) до тех пор, пока не получится единица. Повторяется 100 000 раз. Количество вещественных чисел, необходимых для достижения единицы, должно быть распределено определенным образом.

10. «Тест пересекающихся сумм» (Overlapping Sums Test). Генерируется длинная последовательность на [0, 1). Добавляются последовательности из 100 последовательных вещественных чисел. Суммы должны быть нормально распределены с характерной медианой и сигмой.

11. «Тест последовательностей» (Runs Test). Генерируется длинная последовательность на [0, 1). Подсчитываются восходящие и нисходящие последовательности. Числа должны удовлетворять некоторому распределению.

12. «Тест игры в кости» (The Craps Test). Играется 200 000 игр в кости, подсчитываются победы и количество бросков в каждой игре. Каждое число должно удовлетворять некоторому распределению.

Тесты из батареи Диехарда требуют, чтобы на вход был подан большой файл (более 11 Мб), который содержит случайные целые двоичные числа.

Большинство тестов возвращает так называемое *p*-значение, которое должно быть однородно на [0, 1), если входной файл содержит действительно независимые случайные биты. Эти *p*-значения получены из выражений $p = F(X)$, где F – принятое распределение случайной переменной X. Обычно *p*-значения для случайной величины располагаются в диапазоне от 0,025 до 0,975.

При этом предполагается, что F задает только асимптотическое приближение, для которого пригодными значениями будут и худшие значения на концах интервала. Таким образом, возможны случайные значения величины p, близкие к 0 или 1, типа 0.0012 или 0.9983.

Когда часть входного потока действительно неслучайна, значение p близкое к 0 или 1, будет получено в шести или более местах. Поэтому, если встретилось значение $p < 0.025$ или $p > 0.975$, то не следует сразу делать вывод, что генератор псевдослучайных чисел «провалил испытание на доверительном уровне вероятности 0.05».

И с п о л ь з о в а н и е:

- запустите программу DIEHARD.EXE;
- введите имя файла, содержащего двоичные данные (размер файла должен быть не менее 11 Мб);
- введите имя текстового файла, в который программа должна поместить результат;
- введите подряд 15 символов «1», означающих, что вы хотите выполнить все из 15 тестов.

После окончания работы программы просмотрите полученный текстовый файл и оцените результаты.

Пример 1.1

Первый тест выдал:

```
BIRTHDAY SPACINGS TEST
…
The 9 p-values were
        .242155   .215332   .409381   .354095   .872947
        .233062   .311486   .154540   .862131
  A KSTEST for the 9 p-values yields  .732411
```

Все результаты находятся в пределах $0.025 < p < 0.975$, следовательно, последовательность прошла испытания на случайность для этого теста:

```
This is the MINIMUM DISTANCE test
            for random integers in the file out.bin
   Sample no.    d^2     avg     equiv uni
         5    1.5952   1.5472     .798746
        10    1.2017   1.2026     .701124
        15    3.9543   1.4901     .981206
        20     .1644   1.4644     .152315
        25     .1076   1.4183     .102472
        30    1.3152   1.2843     .733342
        35    1.5188   1.2278     .782682
        40    1.8259   1.3241     .840396
        45    1.3176   1.3282     .733998
        50     .0866   1.2443     .083322
        55    1.4631   1.2583     .770168
        60     .7246   1.2362     .517238
        65    2.9113   1.2086     .946385
        70     .7005   1.2381     .505427
        75     .1027   1.2186     .098026
        80     .5791   1.1725     .441213
        85     .6604   1.1690     .485088
        90     .6227   1.1295     .465185
        95    1.7329   1.1027     .824757
       100     .8229   1.1220     .562677
   MINIMUM DISTANCE TEST for out.bin
        Result of KS test on 20 transformed mindist^2's:
                                 p-value= .639196
```

Хотя в одном случае $p = 0.981206$ не попадает в интервал $0.025 < p < 0.97$, тем не менее в остальных случаях результаты находятся в нужных пределах, следовательно, последовательность прошла испытания на случайность для этого теста и т. д.

Если последовательность прошла испытания для всех тестов батареи, то можно сделать вывод, что датчик генерирует качественную псевдослучайную последовательность.

Если последовательность не прошла хотя бы один из тестов, то можно сделать вывод, что последовательность не является случайной.

Задание для самостоятельной работы

1. В программе «Expert» проверьте случайность файлов, содержащих программный код (.exe) и архивы (.rar, .zip, и т. д.).

Сформулируйте выводы.

2. С помощью программных средств (MS Visual Studio, Borland и. т. д.) написать программу, использующую для генерации датчик псевдослучайных чисел, встроенный в эти средства.

Пример 1.2. Для C++:

```
#define BUFOUTSIZE 20000000

int APIENTRY WinMain(HINSTANCE hInstance,
                     HINSTANCE hPrevInstance,
                     LPSTR     lpCmdLine,
                     int       nCmdShow)
{
     FILE * out;
     DWORD i, dwRand;
     BYTE * hMem = 0;
     try{
          out = fopen("rand_out.bin","wb");
          if (out == NULL) return -1;
          hMem = (BYTE *) ::VirtualAlloc(0, BUFOUTSIZE,
MEM_COMMIT,PAGE_READWRITE);
          if (hMem){
               srand(0);
               for (i= 0; i< BUFOUTSIZE; i++) {
                    dwRand = rand();
                    memcpy( hMem + i,(BYTE *) &dwRand,  1);
               }
               fwrite(hMem,1, BUFOUTSIZE,out);
               ::VirtualFree(hMem,0,MEM_RELEASE);
          }
     }
     catch(...){
          printf("\r\n\error create file");
     }
     fclose(out);
     return 0;
}
```

Выполните анализ полученной последовательности.

Сделайте вывод о качестве встроенного генератора.

3. Воспользовавшись функцией CryptoAPI (<Wincrypt.h>) *CryptGenRandom*, сгенерируйте файл, содержащий псевдослучайные последовательности.

Пример 1.3. Для C++:

```
     DWORD cbGoop = 1000;
     BYTE lpGoop[1000];

  HCRYPTPROV m_hProv;
  m_hProv = NULL;
     ::CryptAcquireContext(&m_hProv, NULL,NULL,
PROV_RSA_FULL,CRYPT_VERIFYCONTEXT);
     if (m_hProv == NULL)
          throw GetLastError();
  if (!CryptGenRandom(m_hProv, cbGoop, lpGoop))
          printf("\r\n\ошибка генерации данных");
  if (m_hProv) ::CryptReleaseContext(m_hProv, 0);
```

Выполните анализ полученной последовательности. Сделайте вывод о качестве криптографического генератора.

4. Самостоятельно реализуйте один из ГСЧ (1.1) – (1.4). С помощью реализованного датчика псевдослучайных чисел создайте файл, содержащий псевдослучайные последовательности. С помощью программы Expert и батареи тестов Диехарда (при положительных результатах) оцените качество сгенерированной последовательности. Сделайте вывод о качестве генератора.

ЛАБОРАТОРНАЯ РАБОТА №2
ПРОСТЕЙШИЕ АЛГОРИТМЫ ШИФРОВАНИЯ

Теоретические сведения

Криптография – достаточно древняя наука, которая прошла большой путь от интуитивных представлений до совершенных математических моделей. Она и сегодня находится в состоянии развития, и будет еще много новых удивительных открытий в этой отрасли знаний. Всю историю криптографии принято делить на три отрезка времени: до опубликованных в 1949 г. работ американского криптографа Клода Шеннона – основоположника теории современной криптографии; период (с 1949 г. по 1976 г.) дальнейшего развития симметричных систем шифрования; и после 1976 г. – период появления асимметричных систем шифрования с открытым ключом шифрования.

В данной лабораторной работе исследуются простейшие шифры дошеннновского периода развития криптографии.

Шифры перестановки

Эти шифры, наверное, являются самыми древними из всех шифров. В таких шифрах символы исходного открытого текста переставляются по определенному правилу. В качестве примера рассмотрим шифр простой перестановки, который использует шифрующие таблицы. В шифрующую таблицу (табл. 2.1) по вертикали без пробелов записывается исходное сообщение:

Я ПРИДУ ЗА ТОБОЙ ВОСЕМЬ ВЕЧЕРА,

а считывание шифртекста происходит по горизонтали:

ЯУБСЕПЗОЕЧРАЙМЕИТВЬРДООВА.

Таблица 2.1

Я	У	Б	С	Е
П	З	О	Е	Ч
Р	А	Й	М	Е
И	Т	В	Ь	Р
Д	О	О	В	А

Ключом в данном методе шифрования является размер таблицы и правило считывания букв. Расшифровка сообщения происходит в обратном порядке: шифртекст разбивается на блоки длиной, равной длине строки, затем эти блоки записываются один под другим с последующим вертикальным считыванием:

Я ПРИДУ ЗА ТОБОЙ ВОСЕМЬ ВЕЧЕРА.

Шифры замены

В этих шифрах символы исходного открытого текста заменяются символами входного или другого алфавита по некоторому оговоренному правилу. В шифрах простой замены замена происходит на символы алфавита исходного текста (одноалфавитная подстановка).

Полибианский квадрат. За два века до нашей эры греческий писатель и историк Полибий изобрел для целей шифрования квадратную таблицу 5×5, заполненную случайным образом 24 буквами греческого алфавита и пробелом (табл. 2.2).

Таблица 2.2

λ	ε	υ	ω	γ
ρ	ζ	δ	σ	ο
μ	η	β	ξ	τ
ψ	π	θ	α	κ
χ	ν	<пробел>	ϕ	ι

При шифровании находилась буква в таблице и заменялась на букву ниже в том же столбце. Если буква находилась внизу столбца, то она заменялась на верхнюю букву этого же столбца. Очевидно, ключом здесь является сама таблица.

Система шифрования Цезаря. В качестве другого примера рассмотрим одну из древнейших систем шифрования – систему шифрования Гая Юлия Цезаря, известного римского императора-полководца (около 50 г. до нашей эры).

В этой системе каждая буква исходного текста заменяется на букву этого же алфавита, которая является циклически смещенной на *K* букв вправо по длине алфавита. В шифре Цезаря это смещение было равно 3 (табл. 2.3). Значение *K* есть ключ этого шифра. Интересно отметить, что Цезарь никогда не ме-

нял значения ключа. В период жизни Цезаря всеобщая неграмотность населения вселяла уверенность в невозможности постичь написанное в виде шифртекста. В табл. 2.3 иллюстрируются одноалфавитные замены в шифре Цезаря.

Известное выражение Цезаря «VENI, VIDI, VICI» («Пришел, увидел, победил») в виде шифртекста будет выглядеть как «YHQL, YLGL, YLFL».

Таблица 2.3

A→D	J→M	S→V
B→E	K→N	T→W
C→F	L→O	U→X
D→G	M→P	V→Y
E→H	N→Q	W→Z
F→I	O→R	X→A
G→J	P→S	Y→B
H→K	Q→T	Z→C
I→L	R→U	–

Задание для самостоятельной работы

Вариант 1 (с использованием программирования)

1. Реализовать программу шифрования (зашифрование и расшифрование) по одному из алгоритмов:

- шифр простой перестановки, который использует шифрующие таблицы (ключ – размер таблицы);
- систему шифрования Гая Юлия Цезаря (ключом является буква алфавита).

2. Реализовать программу дешифрования (подбора ключа или нахождения исходного текста) на основе известного шифртекста.

3. Ответить на вопрос: что можно сделать для увеличения стойкости шифра перестановки, использующего шифрующие таблицы?

4. Сделать вывод о сложности подбора пароля.

5. Оформить отчет (краткий текст и программы).

Вариант 2 (без использования программирования)

1. Зашифровать с помощью шифрующей таблицы какую-либо фразу.

2. Расшифровать фразу (шифр, использующий шифрующую таблицу):

а) **ЗМПАИМРЯАНИ·ИЕИР·ИПНРЧШ!·АРГЮЧ·Е·И·ЫЫЧКОИУЯМЬЛЕРМУ·ТФ·СИТЗЫФ;**

б) **АОУАПОФБОРН·ЧПБС·ТИАНЕАИА·О·ЙСШТЧПТКНАРМЫО·И·СВСЛПЕМРЙРЛЙЕО.**

3. Ответить на вопрос: что можно сделать для увеличения стойкости шифра перестановки, использующего шифрующие таблицы.

4. Оформить отчет.

ЛАБОРАТОРНАЯ РАБОТА №3
ТЕОРИЯ ЧИСЕЛ, КЛАССЫ ВЫЧЕТОВ

Теоретические сведения

Будем рассматривать **N** – множество натуральных чисел; **Z** – множество целых чисел. Множество целых чисел **Z** – счетное, состоит из элементов 0; ±1; ±2; …; ±*n*, … . На нем определены две алгебраические операции – сложение и умножение.

Эти операции обладают следующими свойствами (для любых чисел $a, b, c \in Z$):

- ассоциативность: $a + (b + c) = (a + b) + c$; $a \cdot (b \cdot c) = a \cdot (b \cdot c)$;
- коммутативность: $b + a = a + b$; $a \cdot b = b \cdot a$;
- существует нейтральный элемент 0 для операции сложения и 1 соответственно для умножения: $a + 0 = 0 + a = a$; $a \cdot 1 = 1 \cdot a = a$;
- $(a + b) \cdot c = a \cdot c + b \cdot c$ – закон дистрибутивности;
- для каждого целого $a \in Z$ существует единственное противоположное, т. е. такое целое *b*, что $a + b = b + a = 0$.

Для целых чисел выполняется следующая теорема.

Теорема 3.1 (теорема о делении с остатком). Для любых целых чисел *a* и *b*, $b \neq 0$, существует единственная пара целых чисел *q* и *r*, где $0 \le r < |b|$, так, что $a = b \cdot q + r$.

В этом равенстве *r* называют остатком, а *q* – частным (неполным частным при $r \neq 0$) от деления *a* на *b*. При $r = 0$ величины *b* и *q* называют делителями или множителями числа *a*. Частное и остаток легко найти методом деления уголком.

Следствие. Пусть *b* – натуральное число, $b > 1$. Для всякого целого числа *a* и максимального целого $m \ge 0$ с условием $a > b^m$ существуют единственные целые a_i, $0 \le i < b$, такие, что $a = \pm(a_m b^m + a_{m-1} b^{m-1} + \ldots + a_0)$.

Такое равенство записывают сокращенно $a = \pm(a_m a_{m-1} \ldots a_0)_b$ или $a = \pm a_m a_{m-1} \ldots a_0$ (если b известно по контексту) и называют записью числа a в b-ичной позиционной системе счисления или системе счисления по основанию b.

Для человека кажется естественной привычная десятичная позиционная система записи целых чисел $(b = 10)$. В различных ситуациях более удобными оказываются другие основания. Например, в большинстве компьютеров на микроуровне вычисления проводятся в двоичной системе счисления. Для перехода к ней с десятичной применяют промежуточную – 16-ричную систему счисления.

Лемма 3.1. Если в равенстве $a_1 + a_2 + \ldots + a_n = b_1 + b_2 + \ldots + b_m$ все слагаемые целые числа и все, кроме, может быть, одного делятся на целое d, то и это исключенное слагаемое делится на d.

Определение 3.1. Если целые числа a, a, …, a делятся на целое d, то d называют их общим делителем.

В дальнейшем речь идет только о положительных целых делителях.

Определение 3.2. Максимальный из общих делителей целых чисел a, a, …, a называется их наибольшим общим делителем и обозначается через НОД(a, a, …, a).

Теорема 3.2. Если $a = b \cdot q + c$, то НОД(a, b) = НОД(b, c).

Теорема 3.2 позволила Евклиду (примерно 2300 лет тому назад) обосновать следующий факт.

Теорема 3.3. Наибольший общий делитель целых чисел a и b ($a > b$) равен последнему отличному от нуля остатку цепочки равенств:

$a = b \cdot q_1 + r_1$;

$b = r_1 \cdot q_2 + r_2$;

……

$r_{n-2} = r_{n-1} \cdot q_n + r_n$;

$r = r \cdot q$,

т. е. $r = \text{НОД}(a, b)$.

Теорема 3.3 формулирует алгоритм Евклида для нахождения наибольшего общего делителя целых чисел. Его вариантом является следующий – второй способ вычисления наибольшего общего делителя по алгоритму Евклида – вычисляем последовательно разности $a - b = c$; $b - c = d$; ... до получения последней ненулевой разности, которая и совпадает с НОД(a, b).

Пример 3.1. С помощью алгоритма Евклида найти НОД(72, 26).

Р е ш е н и е. В соответствии с теоремой 3.3

$72 = 26 \cdot 2 + 20$; $26 = 20 \cdot 1 + 6$; $20 = 6 \cdot 3 + 2$; $6 = 2 \cdot 3$.

Следовательно, НОД(72, 26) = 2.

Теорема 3.4. Если d = НОД(a, b), то существуют такие целые u и v, что выполняется следующее соотношение (Безу): $d = au + bv$.

Пример 3.2. Из примера 3.1 следует, что

$$2 = 20 + 6 \cdot (-3) = 20 + (26 + 20 \cdot (-1)) \cdot (-3) = 20 \cdot 4 + 26 \cdot (-3) =$$

$$= (72 + 26 \cdot (-2)) \cdot 4 + 26 \cdot (-3) = 72 \cdot 4 + 26 \cdot (-11).$$

Такой способ получения соотношения Безу для конкретных целых чисел называется расширенным алгоритмом Евклида (блок-схема приведена на рис. 3.1).

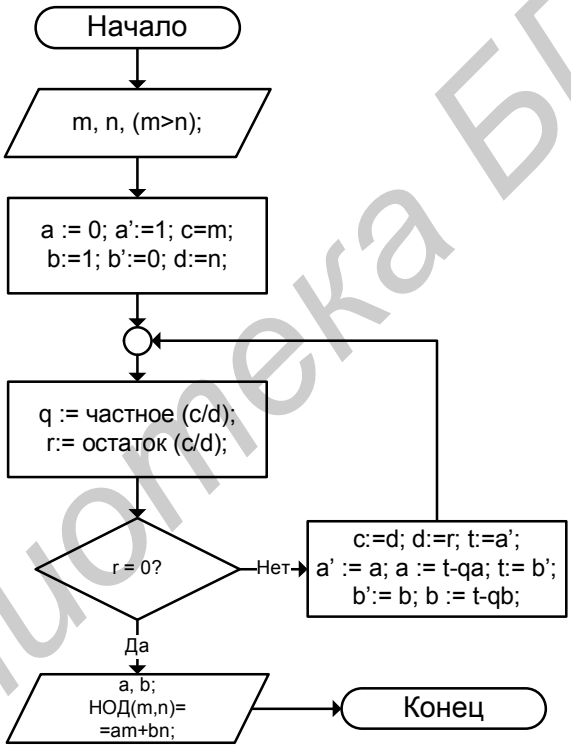

Рис. 3.1. Блок-схема расширенного алгоритма Евклида

Он состоит из двух этапов: прогонки вниз (собственно алгоритма Евклида) и прогонки вверх – последовательного выражения остатков в каждом из шагов предыдущего этапа (с соответствующим приведением подобных на каждом шаге).

Определение 3.3. Натуральное число $p > 1$ называется простым, если оно делится только на единицу и на себя.

Теорема 3.5. Всякое натуральное число $n > 1$либо является простым числом, либо имеет простой делитель.

Заметим, что из соотношения $n = p \cdot q$ натуральных чисел, больших единицы, следует, что либо p, либо q принадлежит отрезку $\left[2;\ \sqrt{n}\right]$. Легко видеть, что наименьший натуральный делитель $p > 1$ натурального числа $n > 1$ является простым числом. Исторически первый метод проверки натурального числа $n > 1$ на простоту заключается в делении его на простые числа, не превосходящие $\sqrt{n}$, носит название «решета Эратосфена». К настоящему времени разработан достаточно большой цикл алгоритмов проверки числа на простоту.

Теорема 3.6 (теорема Евклида). Простых чисел бесконечно много.

Значение теоремы Евклида в том, что простые числа по теореме 3.5 являются составными кирпичиками всех натуральных чисел.

Определение 3.4. Целые числа a и b называются взаимно простыми, если НОД(a, b) = 1.

Теорема 3.7 (критерий взаимной простоты целых чисел). Целые числа a и b взаимно просты тогда и только тогда, когда существуют такие целые u и v, что выполняется равенство $a \cdot u + b \cdot v = 1$.

Следствие. НОД(ac, b) = 1 тогда и только тогда, когда НОД(a, b) = 1 и НОД(c, b) = 1.

Важным в теории чисел и ее приложениях является следующее свойство взаимно простых целых чисел.

Лемма 3.2 Пусть произведение целых чисел ab делится на целое число c и НОД(a, c) = 1. Тогда b делится на c.

Теорема 3.8 (основная теорема арифметики). Всякое целое число $n > 1$ однозначно раскладывается в произведение простых множителей

$n = \pm p \cdot p \cdot \ldots \cdot p$.

Если в этом равенстве собрать одинаковые множители, то получим каноническое разложение целого числа: $n = p \cdot p \cdot \ldots p$.

Пример 3.3 Приведем примеры канонических разложений целых чисел: а) $196 = 2 \cdot 98 = 2 \cdot 2 \cdot 49 = 2^2 \cdot 7^2$; б) $2^{12} - 1 = 4095 = 3^2 \cdot 5 \cdot 7 \cdot 13$.

Теорема 3.9. Пусть m – натуральное число, $m > 1$. Для любых целых чисел a и b следующие условия равносильны:

1) a и b имеют одинаковые остатки от деления на m;

2) $a - b$ делится на m, т. е. $a - b = mq$ для подходящего целого q;

3) $a = b + mq$ для некоторого целого q.

Определение 3.5. Целые числа a и b называются сравнимыми по модулю m, если они удовлетворяют одному из условий теоремы 3.9. Этот факт обозначают формулой $a \equiv b(\mathrm{mod}\, m)$ или $a \equiv b(m)$, и называют данную формулу **сравнением**.

Пример 3.4. $-5 \equiv 7(\mathrm{mod}\ 4) \equiv 11(\mathrm{mod}\ 4) \equiv 23(\mathrm{mod}\ 4) \equiv 3(\mathrm{mod}\ 4)$.

Пример 3.5. Если $a = mq + r$, то $a \equiv r(\mathrm{mod}\, m)$ – всякое целое число сравнимо по модулю m со своим остатком от деления на m. Это следует из определения 3.5 и второго условия теоремы 3.9. Ведь $a - r$ делится на m.

Основные свойства сравнений:

1. Пусть $a \equiv b(\mathrm{mod}\, m)$. Тогда $(a \pm c) \equiv (b \pm c)(\mathrm{mod}\, m)$ для всякого целого c, т. е. к обеим частям сравнения можно добавить (или вычесть из обеих частей) одно и то же число.

2. Сравнения можно почленно складывать и вычитать: если $a \equiv b(\mathrm{mod}\, m)$, $c \equiv d(\mathrm{mod}\, m)$, то $(a + c) \equiv (b + d)(\mathrm{mod}\, m)$; $(a - c) \equiv (b - d)(\mathrm{mod}\, m)$.

3. Сравнения можно почленно перемножать: если $a \equiv b(\mathrm{mod}\, m)$, $c \equiv d(\mathrm{mod}\, m)$, то $ac \equiv bd(\mathrm{mod}\, m)$.

4. Сравнения можно почленно возводить в любую натуральную степень: если $a \equiv b(\mathrm{mod}\ m)$, то $a^n \equiv b^n\ (\mathrm{mod}\ m)$.

5. Если в сравнении $a \equiv b(\mathrm{mod}\ m)$ числа a, b, m имеют общий множитель d, то на него сравнение можно сократить: $a/d \equiv b/d\ (\mathrm{mod}\ m/d)$.

6. Сравнение можно сократить на общий множитель, взаимно простой с модулем: если $a = da_1$ и $b = db_1$, НОД (d, m)=1, то из сравнения $da_1 \equiv db_1(\mathrm{mod}\, m)$ следует сравнимость a_1 и b_1 по модулю m: $a_1 \equiv b_1(\mathrm{mod}\, m)$.

7. Сравнение можно умножить на любой целый множитель: если a≡b(mod m), то $at \equiv bt(\mathrm{mod}\, m)$ для всякого целого t.

8. Рефлексивность: $a \equiv a(\mathrm{mod}\, m)$ для любого целого a и всякого натурального $m > 1$.

9. Симметричность: если $a \equiv b(\mathrm{mod}\ m)$, то $b \equiv a(\mathrm{mod}\ m)$.

10. Транзитивность: если $a \equiv b(\mathrm{mod}\ m)$, $b \equiv c(\mathrm{mod}\ m)$, то $a \equiv c(\mathrm{mod}\ m)$.

Теорема 3.10 (малая теорема Ферма). Пусть p – простое число, целое число a не делится на p. Тогда $a^{p-1} \equiv 1(\mathrm{mod}\, p)$.

Теория сравнений и малая теорема Ферма позволяют быстро находить остаток от деления большого числа на простое число.

Пример 3.6. Найдем остаток от деления 39^{29} на 31.

Р е ш е н и е. $39 \equiv 8 \pmod{31}$. Поэтому в силу 4-го свойства сравнений $39^2 \equiv 8^2 \pmod{31} \equiv 2 \pmod{31}$.

Двоичная запись числа: 29 = 11101. Следовательно, для любого натурального числа a величина $a^{29} = a^{2^4} \cdot a^{2^3} \cdot a^{2^2} \cdot a$.

Далее, $39^4 \equiv 8^4 \pmod{31} \equiv 2^4 \pmod{31}$. Поэтому $39^8 = (39^4)^2 \equiv 4^2 (\mathrm{mod} 31)$. Тогда $39^{16} = (39^8)^2 \equiv 16^2 (\mathrm{mod} 31) \equiv 8 (\mathrm{mod} 31)$.

Следовательно, $39^{29} \equiv 8 \cdot 16 \cdot 4 \cdot 8 (\mathrm{mod} 31) \equiv 4 \cdot 4 \cdot 8 (\mathrm{mod} 31) \equiv 4 (\mathrm{mod} 31)$. Таким образом, остаток от деления 39^{29} на 31 равен 4.

При делении целых чисел на натуральное целое $m > 1$ существует m различных остатков: 0, 1, 2, ..., $m-1$. Соответственно этим остаткам множество **Z** разбивается на m непересекающихся классов сравнимых друг с другом чисел, т. е. имеющих один и тот же остаток от деления на m. В соответствии с остатками от деления на m эти классы будем обозначать через $\bar{0}, \bar{1}, \ldots, \overline{m-1}$. Таким образом, класс $\bar{i} = \{mq + i \mid q \in Z\}$ для каждого целого i = 0, 1, …, m – 1. Любой представитель класса однозначно определяет свой класс: для каждого натурального числа $mq + i$ класс $\overline{mq+i}$. Поскольку остаток – по-латински «residu» – переводится на русский как вычет, то множество всех классов по данному модулю сравнимых друг с другом чисел называют множеством классов вычетов по модулю m и обозначают через Z/mZ. В силу сказанного $Z/mZ = \{\bar{0}, \bar{1}, ..., \overline{m-1}\}$ – множество из m элементов. Заметим, что для любых классов $\bar{k}, \bar{l} \in Z/mZ$ и для произвольных $k, k \in \bar{k}$, $l_1, l_2 \in \bar{l}$ суммы $k_1 + l_1$ и $k_2 + l_2$ принадлежат одному классу из Z/mZ, так как эти суммы сравнимы друг с другом по модулю m согласно 2-му свойству сравнений. Аналогично произведения $k_1 \cdot l_1$ и $k_2 \cdot l_2$ лежат в одном классе из Z/mZ.

Определим операции сложения на *Z*/*mZ*. Полагаем суммой $\bar{k} + \bar{l}$ такой единственный класс $\bar{z}$ из *Z*/*mZ*, в который попадают все суммы $k_1 + l_1$ и $k_2 + l_2$ для $k, k \in \bar{k}$, $l, l \in \bar{l}$, а произведением $\bar{k}\,\bar{l}$ – тот класс из *Z*/*mZ*, в который попадают произведения $\tilde{k} \cdot \tilde{l}$ для $\tilde{k} \in \bar{k}, \tilde{l} \in \bar{l}$.

Примечание. При записи произведения $a \cdot b$ символ операции умножения «·» часто опускают и записывают просто ab.

Поскольку сложение и умножение в Z/mZ однозначно определяются умножением представителей классов, то свойства 1 – 5 операций сложения и умножения целых чисел справедливы и в Z/mZ:

1) $\bar{k}+\bar{l}=\bar{l}+\bar{k}$; $\bar{l}\cdot\bar{k}=\bar{k}\cdot\bar{l}$ – коммутативность;

2) $\bar{k}+(\bar{l}+\bar{r})=(\bar{k}+\bar{l})+\bar{r}$; $\bar{k}\cdot(\bar{l}\cdot\bar{r})=(\bar{k}\cdot\bar{l})\cdot\bar{r}$ – ассоциативность;

3) существует нейтральный элемент: $\bar{k}+\bar{0}=\bar{k}$; $\bar{k}\cdot\bar{1}=\bar{k}$;

4) $(\bar{k}+\bar{l})\cdot\bar{r}=(\bar{k}\cdot\bar{r})\times(\bar{l}\cdot\bar{r})$ – дистрибутивность;

5) для всякого $\bar{k}\in Z/mZ$ существует единственный класс $\bar{l}$, такой, что $\bar{k}+\bar{l}=\bar{0}$ (им является $\bar{l}=\overline{m-k}$).

Благодаря отмеченным свойствам операций сложения и умножения множество Z/mZ в алгебре относят к классу коммутативных колец с единицей (более подробно они будут рассмотрены в других лабораторных работах) и называют кольцом классов вычетов по модулю m.

Определение 3.6. Класс $\bar{k}\in Z/mZ$ называется обратимым, если найдется такой класс $\bar{l}\in Z/mZ$, что $\bar{k}\cdot\bar{l}=\bar{1}$. Тогда класс $\bar{l}$ называют обратным к классу $\bar{k}$.

Из ассоциативности умножения в кольце Z/mZ вытекает, что если $\bar{k}$ обратимый класс, то обратный класс определен однозначно.

Лемма 3.3. Пусть $\bar{k}\in Z/mZ$ такой класс, что $(k,m)=1$. Тогда:

1) для каждого $\bar{l}\neq\bar{0}$ произведение $\bar{k}\cdot\bar{l}\neq\bar{0}$;

2) $\bar{k}\cdot\bar{l}_1\neq\bar{k}\cdot\bar{l}_2$, если $\bar{l}_1\neq\bar{l}_2$;

3) отображение $f:\bar{x}\to\bar{k}\cdot\bar{x}$ инъективно и, следовательно, биективно на множестве Z/mZ (на множестве ненулевых элементов из Z/mZ);

4) $\bar{k}$ – обратимый класс в кольце Z/mZ.

Замечание. По условию леммы 3.1 $\text{НОД}(k,m)=1$, поэтому согласно критерию взаимной простоты целых чисел существуют такие целые u, $v\in Z$, что $k\cdot u+m\cdot v=1$. Тогда $\bar{1}=\bar{k}\cdot\bar{u}+\bar{m}\cdot\bar{v}=\bar{k}\cdot\bar{u}$. Следовательно, $\bar{u}$ – обратный к $\bar{k}$ класс.

Лемма 3.4. Пусть $\bar{k}\in Z/mZ$ такой класс, что $\text{НОД}(k,m)=d>1$. Тогда:

1) существует класс $\bar{l}\cdot\bar{0}$, что $\bar{k}\cdot\bar{l}=\bar{0}$;

2) существуют классы $\bar{l}_1\neq\bar{l}_2$, такие, что $\bar{k}\cdot\bar{l}_1=\bar{k}\cdot\bar{l}_2$;

3) для всех $\bar{l}\cdot\bar{0}$ произведение $\bar{k}\cdot\bar{l}\cdot\bar{1}$, т. е. класс $\bar{l}$ не обратим в кольце Z/mZ.

Теорема 3.11. Класс $\bar{k}$ из кольца Z/mZ обратим тогда и только тогда, когда НОД$(k, m) = 1$. Если $m = p$ – простое число, то в кольце Z/mZ каждый ненулевой класс обратим. Обратный класс также обратим. Произведение обратимых классов есть обратимый класс.

Поскольку Z/mZ состоит из конечного множества элементов, то сложение и умножение можно задавать поэлементно в виде таблиц.

Пример 3.7. Напишем таблицы сложения и умножения в $Z/3Z$ (рис. 3.2).

$\oplus$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

$\otimes$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{1}$

Рис. 3.2. Таблицы сложения и умножения

Из таблицы умножения непосредственно видно, что классы $\bar{1}$ и $\bar{2}$ обратны сами себе, т. е. обратимы все ненулевые классы $Z/3Z$ в полном соответствии с теоремой 3.1.

Определение 3.7. Функция Эйлера – функция натурального аргумента $\varphi(m)$, которая каждому натуральному числу $m > 1$ ставит в соответствие количество натуральных чисел, меньших m и взаимно простых с m.

Перечислим основные мультипликативные свойства функции Эйлера.

Свойство 1. $\varphi(p) = p - 1$ для каждого простого числа p.

Свойство 2. $\varphi(p^n) = p^n - p^{n-1}$ для каждого простого числа p и для произвольного натурального $n \geq 1$.

Свойство 3. Если НОД$(n, m) = 1$ то $\varphi(n \cdot m) = \varphi(n) \cdot \varphi(m)$.

Свойство 4. Если $n = p_1^{s_1} \cdot p_2^{s_2} \cdot \ldots \cdot p_t^{s_t}$ – каноническое разложение числа n, то

$$\varphi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_t}\right).$$

Пример 3.8. Вычислим $\varphi(48)$. Поскольку $48 = 3 \cdot 2^4$, то согласно 4-му свойству значение $\varphi(48) = 48 \cdot (1 - 1/3) \cdot (1 - 1/2) = 16$.

Пример 3.9. Из теоремы 3.11 следует, что в кольце Z/mZ имеется в точности $\varphi(m)$ обратимых классов. Например, $\varphi(12)=4$. Значит, в кольце $Z/12Z$ имеется именно четыре обратимых элемента. Непосредственная проверка показывает, что этими классами являются $\overline{1}, \overline{5}, \overline{7}, \overline{11}$.

Теорема 3.12 (теорема Эйлера). Если для целого числа *a* и натурального *m* $\text{НОД}(a,m)=1,$ то $a^{\varphi(m)} \equiv 1(\text{mod}\, m)$.

Алгебраическим сравнением *n*-й степени с одной неизвестной называется сравнение вида $a_n x^n + a^{n-1} + ... + a_1 x + a_0 x^0 \equiv 0 \,(\text{mod}\, m)$, где $a_n, a_{n-1}, ..., a_0 \in Z$, $n \in N$, $a_n \not\equiv 0(\text{mod}\, m)$.

Если при подстановке вместо *x* числа x_0 получается верное числовое сравнение, то x_0 называется решением данного сравнения. При этом и любое целое число вида $x_0 + mt$ также будет решением данного сравнения. Поэтому решением алгебраического сравнения можно считать класс вычетов $\overline{x_0}$. Универсальным способом решения алгебраических сравнений является испытание полной системы вычетов по модулю *m*, т. е. целых чисел 0, 1, 2, …, *m* – 1. Сравнение будет иметь столько решений, сколько вычетов полной системы ему удовлетворяют.

Пример 3.10. Решить квадратное сравнение $x^2 + x + 1 \equiv 0(\text{mod}\, 7)$.

Р е ш е н и е. Среди чисел 0, 1, 2, 3, 4, 5, 6 полной системы вычетов по модулю 7 удовлетворяют данному сравнению только два числа $x=2, x=4$. Поэтому указанное сравнение имеет два решения: $x \equiv 2(\text{mod}7), \quad x \equiv 4(\text{mod}7).$

При решении сравнений часто используют преобразования, приводящие к равносильным сравнениям.

Примеры решения задач

Задача 3.1. Вычислить $\varphi(n)$ для всех натуральных *n* от 2 до 12.

Р е ш е н и е. Среди чисел от 2 до 12 простыми являются числа 2, 3, 5, 7, 11. Согласно свойству 1 имеем: $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(5) = 4$, $\varphi(7) = 6$, $\varphi(11) = 10$. Так как $4 = 2^2$, $8 = 2^3$ и $9 = 3^2$, то, воспользовавшись свойством 2, получим $\varphi(4) = 2$, $\varphi(8) = 4$ и $\varphi(9) = 6$. Для вычисления функции Эйлера остальных чисел воспользуемся свойством 4: $6 = 3 \cdot 2$, следовательно, $\varphi(6) = 6 \cdot (1 - 1/2) \cdot (1 - 1/3) = 2$; аналогично $\varphi(10) = 4$, $\varphi(12) = 4$.

Задача 3.2. Вычислить $\varphi(60)$, $\varphi(81)$, $\varphi(89)$, $\varphi(2017)$, $\varphi(2018)$.

Р е ш е н и е. $60 = \underset{p_1}{2^2} \cdot \underset{p_2}{3} \cdot \underset{p_3}{5}$. Согласно свойству 4 функции Эйлера

$$\varphi(60) = 60\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right) = 60 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 2 \cdot 2 \cdot 4 = 16,\ 81 = 3^4.$$

Поэтому согласно свойству 2 функции Эйлера

$$\varphi(81) = 3^4 - 3^{3-1} = 3^4 - 3^3 = 81 - 27 = 54.$$

$\sqrt{89} < 10$; 89 не делится на все простые 2, 3, 5, 7, меньшие 10. Следовательно, 89 – число простое. Поэтому $\varphi(89) = 88$.

Задача 3.3. В кольцах $Z/5Z$ и $Z/6Z$ составить таблицы умножения. Найти в этих кольцах пары взаимно обратных по умножению элементов. Указать количество таких пар и сравнить это количество с $\varphi(5)$ и $\varphi(6)$ соответственно.

Р е ш е н и е. $Z/5Z = \{1, 2, 3, 4\}$ и $Z/6Z = \{1, 5\}$,

$\otimes$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

$\varphi(5) = 4$. Пары взаимно обратных элементов по умножению: (1, 1), (2, 3), (3, 2) и (4, 4).

Количество пар взаимно обратных элементов совпадает с $\varphi(5)$.

$\otimes$	$\overline{1}$	$\overline{5}$
$\overline{1}$	$\overline{1}$	$\overline{5}$
$\overline{5}$	$\overline{5}$	$\overline{1}$

$\varphi(6) = 2$. Пары взаимно обратных элементов по умножению: (1, 1) и (5, 5).

Количество пар взаимно обратных элементов совпадает с $\varphi(6)$.

Задача 3.4. В кольце классов вычетов по модулю 15 к каждому обратимому элементу найти обратный элемент.

Р е ш е н и е. Согласно теореме 3.12 в кольце $Z/15Z$ имеется $\varphi(15) = 8$ классов вычетов, взаимно простых с модулем $m = 15$. Эти классы составляют множество $G = \left\{\overline{1}, \overline{2}, \overline{4}, \overline{7}, \overline{8}, \overline{11}, \overline{13}, \overline{14}\right\}$.

С п о с о б 1: на языке сравнений равенство $\overline{a} \cdot \overline{x} = \overline{1}$ для $\overline{a} \in G$ выглядит как $ax \equiv 1 (\mathrm{mod}\, 15)$, а из теоремы Эйлера следует, что $a^8 \equiv 1 (\mathrm{mod} 15)$. Умножив сравнение $ax \equiv 1 (\mathrm{mod}\, 15)$ на a^7, получим $x \equiv a^7 (\mathrm{mod} 15)$ согласно свойствам сравнений. Последовательно вычисляем:

$2^7 = 8 \cdot 16 \equiv 8 (\mathrm{mod}\, 15)$, значит $\left(\overline{2}\right)^{-1} = \overline{8}$;

$4^7 = 16^3 \cdot 4 \equiv 4 (\mathrm{mod}\, 15)$, значит $\left(\overline{4}\right)^{-1} = \overline{4}$;

$7^7 = 49^3 \cdot 7 \equiv 4^3 \cdot 7 \equiv 13, (\overline{7})^{-1} \equiv \overline{13}$;

$11^7 = 121^3 \cdot 11 = 1^3 \cdot 11 \equiv 11(\mathrm{mod}15), (\overline{11})^{-1} = \overline{11}$;

$14^7 = 2^7 \cdot 7^7 \equiv 8 \cdot 13(\mathrm{mod}15) \equiv (-7) \cdot (-2)(\mathrm{mod}15) = 14(\mathrm{mod}15); \quad (\overline{14})^{-1} = \overline{14}$.

С п о с о б 2 (с использованием расширенного алгоритма Евклида): из соотношений Безу имеем

$1 = 15 \cdot 1 + (-7) \cdot 2 \Rightarrow (-7) \cdot 2 \equiv 1(\mathrm{mod}15) \Rightarrow (\overline{2})^{-1} = \overline{-7} = \overline{8}$.

$1 = 15 \cdot (-1) + 4 \cdot 2 \Rightarrow 4 \cdot 2 \equiv 1(\mathrm{mod}15) \Rightarrow (\overline{4})^{-1} = \overline{4}$.

$1 = 15 \cdot 1 + (-2) \cdot 7 \Rightarrow (-2) \cdot 7 \equiv 1(\mathrm{mod}15) \Rightarrow (\overline{7})^{-1} = \overline{-2} = \overline{13}$.

$1 = 15 \cdot 3 + (-4) \cdot 11 \Rightarrow (-4) \cdot 11 \equiv 1(\mathrm{mod}15) \Rightarrow (\overline{11})^{-1} = \overline{-4} = \overline{11}$.

$1 = 15 \cdot 1 + (-7) \cdot 2 \Rightarrow (-7) \cdot 2 \equiv 1(\mathrm{mod}15) \Rightarrow (\overline{2})^{-1} = \overline{-7} = \overline{8}$.

Так как 14 = 15 – 1, а $(m-1)^2 = m^2 - 2m + 1 \equiv 1(\mathrm{mod}m)$, то $(\overline{14})^{-1} = \overline{14}$.

Задача 3.5. Найти обратные к классам $\overline{5}, \overline{6}, \overline{7}$ в кольце:

а) $Z/2017Z$; б) $Z/2018Z$.

Р е ш е н и е. Найдем обратный класс для класса $\overline{5}$ в кольце $Z/2017Z$. Проверим наличие обратного класса (по теореме 3.11): НОД(5, 2017) = 1. Это означает, что обратный класс для $\overline{5}$ в $Z/2017Z$ существует и может быть найден из сравнения $\overline{5} \cdot \overline{x} = \overline{1}$. Так как $\phi(2017) = 2016$, то $x \equiv 5^{2015}(\mathrm{mod}\,2017)$. Тогда x ≡ $5 \cdot 5^{2014}$(mod 2017) ≡ $5 \cdot 25^{1007}$(mod 2017) ≡ $5 \cdot 25 \cdot 625^{503}$(mod 2017) ≡ ≡ $125 \cdot 625^3 \cdot 625^{500}$(mod 2017) ≡ $125 \cdot 928 \cdot 625^{500}$(mod 2017) ≡ $125 \cdot 928 \cdot 726^{100}$(mod 2017) ≡ ≡ $125 \cdot 928 \cdot 539^{20}$(mod·2017) ≡ $125 \cdot 928 \cdot 123^4$(mod 2017) ≡ 125·928·1515(mod·2017) ≡ ≡ 807(mod 2017), т. е. $(\overline{5})^{-1} = \overline{807}$.

Проверим полученный результат: 5·807 = 4035 ≡ 1(mod 2017).

Второй способ основывается на применении расширенного алгоритма Евклида. Запишем соотношения Безу: НОД(5, 2017) = (–2)·2017 + 807·5, т. е. $(\overline{5})^{-1} = \overline{807}$.

Аналогично решается и пункт б.

Задание для самостоятельной работы

1. Написать программу, реализующую алгоритм Евклида и расширенный алгоритм Евклида.

2. Написать программу, реализующую каноническое разложение числа.

3. Найти канонические разложения чисел m и n.

Найти НОД(a, b), воспользовавшись:

а) алгоритмом Евклида;

б) разложением чисел на простые множители.

4. С помощью расширенного алгоритма Евклида найти целые a, b, удовлетворяющие соотношению Безу: $a \cdot m + b \cdot n$ = НОД(m, n). Значения m и n приведены в табл. 3.1.

Таблица 3.1

№ варианта	m	N
1	7672333	48685811
2	660422941	36481301
3	101398751	326147777
4	9002242397	433817903
5	9118515943	3386496689
6	5336161097	196210799

5. Вычислить функции Эйлера $\varphi(k)$, $\varphi(n)$ и $\varphi(m)$ (значения k, n и m взять из табл. 3.2).

6. В кольцах Z/kZ и Z/nZ (значения k и n – определены ниже) найти пары взаимно обратных по умножению элементов.

7. В кольце Z/mZ найти обратные к элементам $\overline{5}$, $\overline{6}$, $\overline{7}$.

Таблица 3.2

№ варианта	k	n	m
1	13	18	2002
2	12	23	2000
3	11	24	2001
4	17	21	2003
5	19	26	2004
6	13	27	2007

ЛАБОРАТОРНАЯ РАБОТА №4
МАТЕМАТИЧЕСКИЕ ОСНОВЫ КРИПТОГРАФИИ

Теоретические сведения

Двумя важными простейшими классами блочных шифров являются подстановочные и перестановочные. Согласно К. Шеннону основными методами маскировки избыточности открытого текста служат перемешивание и рассеивание. Перемешивание существенно усложняет взаимосвязи статистических и аналитических характеристик открытого и шифрованного текста. Рассеивание распространяет влияние отдельных бит открытого текста на как можно большее количество бит шифртекста, что также маскирует статистические взаимосвязи и усложняет криптоанализ. Один из основных приемов состоит в том, чтобы в одном шифре в различных комбинациях периодически перемежать рассеивание (с гораздо меньшими таблицами) и перемешивание. Криптографические функции реализуются посредством комбинации подстановочных и перестановочных преобразований. Обычно перестановочные преобразования являются линейными, а подстановочные – основной источник нелинейности в шифре.

Для анализа криптографических преобразований используются такие разделы математики, как теория групп, колец и полей.

Определение 4.1. Пусть S – некоторое множество, и пусть $S \times S$ – множество упорядоченных пар (s, t), где $s, t \in S$. Тогда произвольное отображение из $S \times S$ в S называется бинарной операцией на множестве S, а множество S с бинарной операцией – алгеброй.

Определение 4.2. Пусть даны алгебры $(M,\cdot)$ и $(M^*,\cdot)$. Алгебры $(M,\cdot)$ и $(M^*,\cdot)$ называются изоморфными, если существует биективное отображение $f : M \to M^*$ такое, что для любых $a, b \in M$ выполняется $f(a \cdot b) = f(a) \cdot f(b)$. Такое отображение f называется изоморфизмом между $(M,\cdot)$ и $(M^*,\cdot)$.

Изоморфные алгебры отличаются друг от друга природой своих элементов и, может быть, названием операции и применяемой символикой. Однако с точки зрения свойств самих операции они неразличимы. Все, что можно доказать для одной алгебры, автоматически переносится на алгебры, изоморфные с ней.

Элементы теории групп – определения

Определение 4.3. Группой $(G, \otimes)$ называется множество G с бинарной операцией «$\otimes$» на нем, для которых выполнены следующие три условия:

• Операция «$\otimes$» ассоциативна, т.е. для любых $a,b,c \in G$ выполняется равенство $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

• В G существует нейтральный элемент e такой, что для любого $a \in G$ выполнено равенство $a \cdot e = e \cdot a = a$.

• Для каждого элемента $a \in G$ существует обратный элемент a^{-1} такой, что выполнено равенство $a \cdot a^{-1} = a^{-1} \cdot a = e$.

О б о з н а ч е н и е: группу обозначают $(G,\cdot)$ либо коротко G.

Теорема 4.1. Если в группе имеется нейтральный элемент, то он один.

Д о к а з а т е л ь с т в о. Если e и e_1 – два нейтральных элемента в группе G, то $e = e \cdot e_1 = e_1$. Теорема доказана.

Утверждение 4.1. Для множества G с ассоциативной операцией «$\otimes$» равносильны следующие условия:

1) $(G, \otimes)$ – группа;

2) для любой пары $a,b \in G$ каждое из уравнений $a \otimes x = b$ и $x \otimes a = b$ имеет единственное решение;

3) для любой пары $a,b \in G$ каждое из уравнений $a \otimes x = b$ и $x \otimes a = b$ имеет хотя бы одно решение.

Определение 4.4. Группа, которая удовлетворяет условию: для любых $a, b \in G$ выполняется равенство $a \otimes b = b \otimes a$, называется абелевой или коммутативной.

Часто для простоты записи групповой операции используют мультипликативное обозначение «·» (как для обычного умножения чисел) и вместо $a \otimes b$ пишут $a \cdot b$, или ab, и называют этот элемент произведением элементов a и b. При этом не предполагается, что операция и в самом деле является умножением. В этом случае часто группу называют мультипликативной, а нейтральный элемент e – единицей и обозначают 1.

Иногда для групповой операции бывает удобно использовать аддитивную запись и писать $a + b$ вместо $a \otimes b$ (и называть этот элемент суммой элементов a и b), 0 вместо e (этот элемент называют **нулем группы** G) и «–a» – вместо a^{-1}.

В этом случае группу часто называют **аддитивной**. Аддитивные обозначения используют, как правило, для абелевых групп.

Пример 4.1. Пусть G – это множество целых чисел Z с обычной операцией сложения «+». Известно, что эта ассоциативная операция является коммутативной. Легко убедиться, что G является коммутативной группой, в которой единичным элементом является 0, а обратным элементом для числа a является противоположное число $-a$.

Пример 4.2. Множество матриц образует группу по сложению.

Пример 4.3. Множество целых чисел не образует группу по умножению, так как обратные для целых чисел (отличных от –1 и 1) не являются целыми числами.

Определение 4.5. Группа (мультипликативная) G называется **циклической**, если в ней существует такой элемент $a \in G$, что любой элемент $b \in G$ является степенью элемента a, т. е. существует целое число k, такое, что $b = a^k$. Такой элемент a циклической группы G называется **образующим** или **порождающим**.

Определение 4.6. Группа называется **конечной** (соответственно **бесконечной**), если она состоит из конечного (соответственно бесконечного) числа элементов. Число элементов группы называется **порядком**.

О б о з н а ч е н и е: порядок группы G обозначается $|G|$ или $\#G$.

Определение 4.7. Подмножество $H \subseteq G$ группы G называют **подгруппой** этой группы $(H \le G)$, если само множество H образует группу относительно операции группы G. Подгруппы группы G, отличные от тривиальных подгрупп $\{e\}$ и G, называются **собственными подгруппами**.

Определение 4.8. Подгруппа группы G, состоящая из всех степеней элемента $g \in G$ этой группы, называется **подгруппой, порожденной элементом** g, и обозначается $\langle g \rangle$. Если $\langle g \rangle$ – конечная циклическая подгруппа, то ее порядок $\#\langle g \rangle$ называется **порядком элемента** g. В противном случае элемент g называется **элементом бесконечного порядка**.

Смежные классы и фактор-группы

Определение 4.9. Если H некоторое непустое подмножество группы G, то подгруппа H группы G, состоящая из всех произведений конечной длины всех степеней из H, называется **подгруппой, порожденной множеством** H, и обозначается $h = \langle H \rangle$, а H называется **множеством образующих подгруппы** h.

Определение 4.10. Если подгруппа h группы G такова, что множество смежных классов G по h конечно, то число этих смежных классов (левых и правых) называется **индексом подгруппы** h **в группе** G и обозначается $(G:h)$.

Теорема 4.2. Пусть элемент $g \in G$ обладает свойством $g^n = e$ для некоторого целого n и $g^k \neq e$ для всех целых $1 \le k < n$. Тогда циклическая группа $\langle g \rangle$ имеет порядок n и $\langle g \rangle = \{g, g^2, ..., g^n = e\}$.

Определение 4.11. Наименьшее натуральное число n (если оно существует), для которого выполнено равенство $g^n = e$ для всех $g \in G$, называется **экспонентой группы** G и обозначается exp$G$. Экспонента конечной группы G делит порядок этой группы, т. е. $0 \equiv |G| \bmod(\exp G)$.

Определение 4.12. Пусть G – произвольная группа, H – ее подгруппа и g – произвольный элемент группы G. Множество $hg = \{hg | h \in H\}$ называется **смежным классом (правым смежным классом)** элемента g.

Введем отношение $g_1 \equiv g_2 (\bmod H)$ на множестве элементов группы G по правилу $g_1 \equiv g_2 (\bmod H)$ в том и только том случае, если $Hg_1 = Hg_2$.

Использование обозначения, сходного с отношением делимости для целых чисел, неслучайно, поскольку отношение делимости является частным случаем равенства смежных классов, если в качестве группы G берется множество $\boldsymbol{Z}$ целых чисел по сложению, а в качестве подгруппы H берется множество kZ чисел, которые делятся на k.

Очевидно, что таким образом определенное отношение является эквивалентностью. Множество классов эквивалентности обозначается через G/H, мощность $|G/H|$ множества классов эквивалентности обозначается еще как $|G:H|$ и называется индексом подгруппы H в группе G. Очевидно, что для любого $g \in G$ справедливо $|Hg| = |H|$, откуда сразу следует теорема Лагранжа: $|G| = |G:H| \Delta |H|$. В частности, порядок подгруппы всегда делит порядок группы.

На множестве G/H можно естественным образом определить операцию умножения:

$$Hg_1 \Delta Hg_2 = H(g_1 \Delta g_2).$$

Для того чтобы определение было корректным, т. е. выполнялись равенства множеств $Hg_1\Delta Hg_2 = \{h_1 g_1 \cdot h_2 g_2 \mid h_1, h_2 \in H\}$ и $Hg_1\Delta g_2 = \{hg_1\Delta g_2 \mid h \in H\}$, необходимо и достаточно, чтобы для любого $g \in G$ выполнялось равенство:

$$g^{-1}Hg = \{g^{-1}hg = h \mid h \in H\} = H$$

(это условие будем коротко записывать $H^G \subseteq H$).

Выражение $g^{-1}Hg$ называется сопряжением с помощью элемента *g* и часто обозначается H^g. Подгруппа *G*, удовлетворяющая условию $H^G \subseteq H$, называется нормальной подгруппой группы *G*, а получившаяся группа G/H называется **фактор-группой** группы *G* по группе *H*.

Понятия нормальной подгруппы и фактор-группы являются одними из важнейших в теории групп, поскольку позволяют частично сводить изучение групп к меньшим группам (частично, так как по данным *H* и *G/H* группа *G* определяется неоднозначно). Группа, не содержащая нормальных групп, называется простой.

Симметрическая группа подстановок

Определение 4.13. Любое взаимно однозначное отображение (биекция) множества Ω в себя называется подстановкой на Ω.

Поскольку природа множества Ω обычно не важна, то при изучении подстановок рассматривают биективные отображения f вида

$$f : \{1, 2, ..., n\} \to \{1, 2, ..., n\}, \text{ где } n \in N.$$

Подстановку f удобно изображать в наглядной развернутой форме в виде двухстрочной таблицы $i_k \in \Omega,\ k = 1, ..., n = |\Omega|;\ i_k \neq i_j, \forall k, j : k \neq j$:

$$f = \begin{pmatrix} i_1 & i_2 & \dots & i_n \\ f(i_1) & f(i_2) & \dots & f(i_n) \end{pmatrix}.$$

В этой таблице каждый *k*-й столбец четко указывает, в какой элемент $f(i_k)$ преобразуется элемент $i_k, 1 \le i_k \le n$. Подстановки перемножаются в соответствии с общим правилом композиции отображений: $(gf)(i) = g(f(i))$.

Чаще всего $gf \neq fg$, т. е. композиция подстановок не обладает свойством коммутативности. Очевидно, тождественная подстановка $e = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$ играет роль единицы относительно композиции подстановок.

Как известно, композиция отображений является ассоциативной операцией, поэтому и композиция подстановок ассоциативна. Каждая подстановка – обратимая операция. Чтобы найти для подстановки f обратную подстановку f^{-1}, достаточно в таблице $\begin{pmatrix} 1 & 2 & \dots & n \\ f(1) & f(2) & \dots & f(n) \end{pmatrix}$ переставить строки местами, а затем столбцы упорядочить по возрастанию элементов первой строки.

Пример 4.4. Рассмотрим следующие подстановки f и g:

$$f = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7 \\ 2\,4\,6\,1\,3\,5\,7 \end{pmatrix} = \begin{pmatrix} 2\,1\,3\,5\,4\,6\,7 \\ 4\,2\,6\,3\,1\,5\,7 \end{pmatrix}, \quad g = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7 \\ 3\,2\,1\,7\,6\,5\,4 \end{pmatrix};$$

$$fg = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7 \\ 2\,4\,6\,1\,3\,5\,7 \end{pmatrix} \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7 \\ 3\,2\,1\,7\,6\,5\,4 \end{pmatrix} = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7 \\ 6\,4\,2\,7\,5\,3\,1 \end{pmatrix};$$

$$gf = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7 \\ 3\,2\,1\,7\,6\,5\,4 \end{pmatrix} = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7 \\ 2\,4\,6\,1\,3\,5\,7 \end{pmatrix} \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7 \\ 2\,7\,5\,3\,1\,6\,4 \end{pmatrix}.$$

Обратной подстановкой к f будет (меняем строки местами и затем упорядочиваем первую строку по возрастанию перестановкой столбцов):

$$f^{-1} = \begin{pmatrix} 2\,4\,6\,1\,3\,5\,7 \\ 1\,2\,3\,4\,5\,6\,7 \end{pmatrix} = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7 \\ 4\,1\,5\,2\,6\,3\,7 \end{pmatrix}.$$

Легко проверить, что $ff^{-1} = f^{-1}f = e = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7 \\ 1\,2\,3\,4\,5\,6\,7 \end{pmatrix}$.

Таким образом, множество всех подстановок на Ω образует группу относительно операции композиции отображений – умножения подстановок. Её называют симметрической группой на n элементах и обозначают через S_n (иногда используется обозначение $S(\Omega)$ – симметрическая группа на элементах из множества Ω).

Теорема 4.3. Порядок группы S_n равен $n!$.

Определение 4.14. Носителем $T(\sigma)$ подстановки $\sigma \in S_n$ называется множество, составленное из всех элементов $a \in \Omega$, для которых $\sigma(a) \neq a$. Элементы множества $\Omega \setminus T(\sigma)$ называют **неподвижными точками** σ. Подстановки $\sigma_1\sigma_2 \in \Omega$ **независимы**, если $T(\sigma_1) \cap T(\sigma_2) = \varnothing$.

Определение 4.15. Циклом длиной k называется подстановка вида

$$f_k = (i, f(i), ..., f^{k-1}(i)) = \begin{pmatrix} i & f(i) & \dots & f^{k-1}(i) \\ f(i) & f^2(i) & \dots & i \end{pmatrix}.$$

Цикл длиной 2 называется транспозицией. Циклы без общих элементов называются независимыми или непересекающимися.

Теорема 4.4. Каждая подстановка $f \in S_n, f \neq e$, является произведением независимых циклов длиной $l \geq 2$. Это разложение в произведение определено однозначно с точностью до порядка следования циклов.

Пример 4.5. Подстановку f из примера 4.4 можно представить в виде

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 4 & 6 & 1 & 3 & 5 & 7 \end{pmatrix} = (1, 2, 4)(3, 6, 5)(7).$$

Очевидно, что каждый из циклов является подстановкой:

$$(1, 2, 4) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 4 & 3 & 1 & 5 & 6 & 7 \end{pmatrix}; \ (3, 6, 5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 6 & 4 & 3 & 5 & 7 \end{pmatrix}; \ (7) = e.$$

Циклы длиной 1 совпадают с единицей (тождественной подстановкой *e*), поэтому они обычно опускаются.

Произведение (композиция) независимых циклов является коммутативной операцией: $f = (1, 2, 4)(3, 6, 5) = (3, 6, 5)(1, 2, 4)$. Для пересекающихся циклов это не верно.

Цикл можно представить в виде произведения транспозиций $(1, 2, 4) = (2, 4)(1, 4)$; $(3, 6, 5) = (5, 6)(3, 5) = (3, 5)(5, 6)$. Такое представление не однозначно!!!

Один и тот же цикл можно записать разными способами:

$(3, 6, 5) = (5, 3, 6) = (6, 5, 3)$.

Теорема 4.5. Каждая подстановка $f \in S_n$ раскладывается в произведение транспозиций. Любые два разложения данной подстановки в произведения транспозиций содержат либо четное число сомножителей, либо нечетное.

Определение 4.16. Подстановка называется четной (нечетной), если ее разложение в произведение транспозиций содержит четное (нечетное) количество сомножителей.

Так как произведение четных подстановок дает четную подстановку, то множество всех четных подстановок из S_n образует группу. Эта группа называется знакопеременной группой степени *n* и имеет порядок, равный $n!/2$.

Для генерации случайной подстановки можно воспользоваться алгоритмом, показанном на рис. 4.1.

ШАГ 1. Для k =1, 2, …, n установить $s_k = 1$.

ШАГ 2 Для $k = n, n-1, \ldots, 2$ выполнить:

а) получить случайное число $r_k \in \{1, 2, ..., n\}$;

б) выполнить транспозицию $s_k \leftrightarrow s_{r_k}$.

Рис. 4.1. Алгоритм генерации случайной подстановки

Теорема 4.6 (теорема Кэли). Всякая конечная группа порядка n изоморфна некоторой подгруппе симметрической группы порядка n.

Циклические группы

Теорема 4.7. Пусть g – фиксированный элемент произвольной мультипликативной группы G. Пусть $\langle g \rangle = \{g^0 = e, g, g^2, ..., g^{-1}, g^{-2}, ...\}$ – множество всевозможных степеней элемента g. Тогда $\langle g \rangle$ – группа, причем абелева.

Замечание $\langle g \rangle$ – подгруппа исходной группы G.

Теорема 4.8. Всякая подгруппа циклической группы также является циклической.

Теорема 4.9. В конечной циклической группе $\langle g \rangle$ порядка n элемент g^r порождает группу порядка n/НОД(n, r).

Рассмотрим алгебру (**Z**, +), где + – обычная операция сложения. Очевидно, что алгебра (**Z**, +) является группой. Пусть $p \in N$, тогда числа $\{0, 1, ..., p-1\}$ разбивают множество **Z** на смежные классы $\bar{0}, \bar{1}, ..., \overline{p-1}$, такие, что $\forall a \in \bar{k}$, выполняется $a \equiv k \bmod p$. Эти смежные классы образуют группу, которая обозначается Z_p. Вместо классов вычетов можно рассматривать множество неотрицательных чисел {0, 1, …, p – 1} с операцией $+$: $a + b \stackrel{def}{=} (a + b) (\bmod p)$. Эта операция введена корректно, так как $(a+b)(\bmod p) = (a(\bmod p) + b(\bmod p))(\bmod p)$. Тогда Z_p называется **полной системой вычетов по модулю** p.

Очевидно, что эта группа является циклической и ее образующей является элемент $\bar{1}$.

Пусть $a, b \in Z$, обозначим $(a, b) = \text{НОД}(a, b)$.

Наибольший интерес представляет подмножество элементов этой группы Z_p, состоящее из классов $\bar{k} \in Z_p : (k, p) = 1$. Введем операции умножения «·» по пра-

вилу: $\overline{a} \cdot \overline{b} \overset{def}{=\!=} a \cdot b \bmod p$. В силу свойств модулярного умножения $(a \cdot b)(\bmod p) = (a(\bmod p) \cdot b(\bmod p))(\bmod p)$, поэтому операция введена корректно. Легко проверить, что полученная алгебра является группой, которая обозначается Z_p^* или Z/pZ и называется **приведенной системой вычетов по модулю** p.

Некоторые свойства приведенной системы вычетов

Из теории известно, что $\forall p \in N$ существует единственное представление в виде произведения простых сомножителей $p_1 < ... < p_k$ в виде $p = \prod_{i=1}^{k} p_i^{S_i}$.

В лабораторной работе №3 дано определение функции Эйлера. На практике удобнее использовать эквивалентное определение этой функции, вытекающее из следствия 4.

Определение 4.17. Функцией Эйлера числа $p = \prod_{i=1}^{k} p_i^{S_i} \in N$ называется целочисленная функция $\phi(p) = p \cdot \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$.

Следующая теорема позволяет определить порядок приведенной системой вычетов по модулю p.

Теорема 4.10. Группа Z_p^* содержит $\phi(p)$ элементов.

Циклические группы используются в криптосистеме RSA и алгоритме открытого распределения ключей Диффи – Хелмана. Для доказательства корректности в этих системах используются приведенные в лабораторной работе №3 теоремы 3.10 (малая теорема Ферма) и 3.12 (теорема Эйлера).

Приведенная система вычетов по модулю p в общем случае не является циклической группой. Следующая теорема дает ответ на вопрос: «Когда Z_m^* является циклической группой?».

Теорема 4.11. Группа Z_m^* является циклической тогда и только тогда, когда $m = 1, 2, 4, p^k, 2p^k$, где p обозначает нечетное простое число, $k \in N$.

Пример 4.6. Рассмотрим $Z_{24}^* = \{1, 5, 7, 11, 13, 17, 19, 23\}$. Эта группа не является циклической, так как $24 = 2^3 \cdot 3$. Действительно:

$5 \cdot 5 = 1 \pmod{24}$, $7 \cdot 7 = 1 \pmod{24}$, $11 \cdot 11 = 1 \pmod{24}$, $13 \cdot 13 = 1 \pmod{24}$,

$17 \cdot 17 = 1 \pmod{24}$, $19 \cdot 19 = 1 \pmod{24}$, $23 \cdot 23 = 1 \pmod{24}$, т. е. каждый элемент является обратным себе.

Определение 4.18. Элемент $g \in Z_p^*$, который является образующим для Z_p^* (в случае, когда эта группа – циклическая), называется первообразным корнем по модулю p.

В алгоритме Диффи – Хелмана требуется выбрать большое простое число p и какой-либо первообразный корень по модулю p.

На вопрос, как находить первообразные корни по модулю p для некоторых случаев, отвечает следующая теорема.

Теорема 4.12. Пусть p – простое число, $p > 2$.

Пусть $p - 1 = \prod_{j=1}^{k} q_j^{\alpha_j}$ есть разложение p – 1 на простые множители. Число g является первообразным корнем по модулю p тогда и только тогда, когда $\text{НОД}(g, p) = 1$ и $g^{(p-1)/q_j} \neq 1 (\text{mod}\, p)$, $j = 1, 2, ..., k$.

Пусть g – первообразный корень по модулю p, число g_1 равно тому из чисел g или $g + p$, которое удовлетворяет сравнению $x^{p-1} \neq 1 (\text{mod}\, p^2)$. Тогда g_1 является первообразным корнем по модулю p^2.

Если число g_2 является первообразным корнем по модулю p^2, то g_2 является первообразным корнем по модулю p^k для всех $k \in N$.

Пример 4.7. Рассмотрим $Z_9^* = \{1, 2, 4, 5, 7, 8\}$. Поскольку $9 = 3^2$, то эта группа является циклической.

Согласно теореме 4.12 образующий элемент g должен быть образующим и для Z_3^*, Z_{27}^*.... Группа $Z_3^* = \{1, 2\}$ и $2 \neq 1 (\text{mod}\, 3)$, при этом $2^{3-1} = 4 \neq 1 (\text{mod}\, 3^2)$. Следовательно, 2 – образующая циклической группы Z_9^*:

$2^1 = 2 (\text{mod}\, 9)$; $2^2 = 4 (\text{mod}\, 9)$; $2^3 = 8 (\text{mod}\, 9)$;

$2^4 \equiv 7 (\text{mod}\, 9)$; $2^5 \equiv 5 (\text{mod}\, 9)$; $2^6 \equiv 1 (\text{mod}\, 9)$.

Поскольку $7 \equiv 1 (\text{mod}\, 3)$ и $4 \equiv 1 (\text{mod}\, 3)$, то 7 и 4 не являются образующими элементами для Z_3^* и Z_9^*:

$4^1 = 4(\mathrm{mod}9);\quad 4^2 \equiv 7(\mathrm{mod}9);\quad 4^3 \equiv 1(\mathrm{mod}9).$

$7^1 = 7(\mathrm{mod}9);\quad 7^2 \equiv 4(\mathrm{mod}9);\quad 7^3 \equiv 1(\mathrm{mod}9).$

$5 = 2 + 3$ *и* $5^2 = 25 \equiv 7(\mathrm{mod}3)$, следовательно, 5 – также образующий элемент Z_9^*:

$5^1 = 5(\mathrm{mod}9);\quad 5^2 \equiv 7(\mathrm{mod}9);\quad 5^3 \equiv 8(\mathrm{mod}9);$

$5^4 = 4(\mathrm{mod}9);\quad 5^5 \equiv 2(\mathrm{mod}9);\quad 5^6 \equiv 1(\mathrm{mod}9).$

Проверим элемент 8. $8^2 \equiv 1(\mathrm{mod}9)$, следовательно элемент 8 не является образующим для группы Z_9^*. Таким образом, только элементы $\{2, 5\}$ являются образующими элементами циклической группы Z_9^*.

Пример 4.8. Пусть $p = 1741$, найти g – первообразный корень по модулю 1741.

Р е ш е н и е. Представим $p - 1$ в виде произведения простых сомножителей:

$1741 - 1 = 1740 = 2^2 \cdot 3 \cdot 5 \cdot 29.$

По теореме 4.12 нужно проверить четыре равенства:

$$\begin{cases} g^{870}(\mathrm{mod}1741) \neq 1(\mathrm{mod}1741), \\ g^{580}(\mathrm{mod}1741) \neq 1(\mathrm{mod}1741), \\ g^{348}(\mathrm{mod}1741) \neq 1(\mathrm{mod}1741), \\ g^{60}(\mathrm{mod}1741) \neq 1(\mathrm{mod}1741). \end{cases}$$

$2^{870} = 2^{2\cdot3\cdot5\cdot29};\Rightarrow 2^{870}(\mathrm{mod}1741) \equiv 483^{30}(\mathrm{mod}1741) \equiv 1736^{15}(\mathrm{mod}1741) \equiv$

$\equiv 1616^5(\mathrm{mod}1741) \equiv 1740(\mathrm{mod}1741) \neq 1(\mathrm{mod}1741);$

$2^{580} = 2^{4\cdot5\cdot29}(\mathrm{mod}1741);\Rightarrow 2^{580}(\mathrm{mod}1741) \equiv 483^{20}(\mathrm{mod}1741) \equiv$

$\equiv 1629^4(\mathrm{mod}1741) \equiv 356(\mathrm{mod}1741) \neq 1(\mathrm{mod}1741);$

$2^{348} = 2^{2\cdot2\cdot3\cdot29} = (2^{29})^{12};\Rightarrow 2^{348}(\mathrm{mod}1741) \equiv 483^{4\cdot3}(\mathrm{mod}1741) \equiv 25^3(\mathrm{mod}1741) \equiv$

$\equiv 1697(\mathrm{mod}1741) \neq 1(\mathrm{mod}1741).$

Следовательно, 2 – образующий элемент.

Задание для самостоятельной работы

1. Выпишите подстановку, обратную f (подстановку взять из табл. 4.1).
2. Найдите произведение подстановок f и g (подстановки взять из табл. 4.1).
3. Найдите произведение подстановок g и f (подстановки взять из табл. 4.1).

4. Представьте подстановки f, g в виде произведения циклов и транспозиций (подстановки приведены в табл. 4.1).

Напишите программу генерации реализаций случайной подстановки $s = (s_1, ..., s_n)$. Можно воспользоваться алгоритмом, показанном на рис. 4.1.

Таблица 4.1

№ варианта	Подстановки
1	$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 7 & 2 & 4 & 6 & 1 & 3 \end{pmatrix}, g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 7 & 3 & 6 & 2 & 5 & 1 \end{pmatrix}$
2	$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 7 & 3 & 6 & 2 & 5 & 1 \end{pmatrix}, g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 1 & 7 & 6 & 5 & 4 \end{pmatrix}$
3	$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 7 & 4 & 1 & 5 & 2 & 6 \end{pmatrix}, g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 1 & 4 & 7 & 3 & 3 & 2 \end{pmatrix}$
4	$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 2 & 5 & 1 & 4 & 7 & 3 \end{pmatrix}, g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 3 & 6 & 2 & 5 & 1 & 4 \end{pmatrix}$
5	$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 1 & 4 & 7 & 3 & 6 & 2 \end{pmatrix}, g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 6 & 4 & 2 & 7 & 5 & 3 \end{pmatrix}$
6	$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 5 & 3 & 1 & 6 & 4 & 2 \end{pmatrix}, g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 6 & 7 & 1 & 2 & 3 & 4 \end{pmatrix}$

5. Проверьте, является ли циклической группа Z_m^* для заданных m (табл. 4.2).

Таблица 4.2

Вариант	1	2	3	4	5	6
m	60 951	32 460	24 334	16 807	23 951	60 800
	493 039	29 791	73 984	117 992	583 039	29 282

6. Найдите все образующие элементы Z_m^* для заданных m (табл. 4.3).

Таблица 4.3

Вариант	1	2	3	4	5	6
m	18	27	11	13	17	14

7. Найдите какой-либо образующий элемент для Z_m^* для заданных m (табл. 4.4).

Таблица 4.4

Вариант	1	2	3	4	5	6
m	2741	2543	2531	1931	2749	1913

ЛИТЕРАТУРА

1. Мао, В. Современная криптография: теория и практика : пер. с англ. / В. Мао. – М. : Изд. дом «Вильямс», 2005. – 768 с.

2. Кнут, Д. Искусство программирования : пер. с англ. Т. 1 : Основные алгоритмы / Д. Кнут. – 3-е изд. – М. : Изд. дом «Вильямс», 2000 – 720 с.

3. Василенко, О. Н. Теоретико-числовые алгоритмы в криптографии / О. Н. Василенко. – М. : МЦНМО, 2003. – 328 с.

4. Diehard Battery of Tests of Randomness [Электронный ресурс]. – Режим доступа : http://www.stat.fsu.edu/pub/diehard/.

5. Харин, Ю. С. Компьютерный практикум по математическим методам защиты информации : учеб. пособие / Ю. С. Харин, С. В. Агиевич. – Минск : БГУ, 2001. – 190 с.

6. Саймон, С. Книга шифров: тайная история шифров и их расшифровки / С. Саймон. – М. : АСТ ; Астрель, 2007. – 447 с.

7. Ван дер Варден, Б. Л. Алгебра / Б. Л. Ван дер Варден. – М. : Наука, 1976. – 648 с.

8. Шеннон, К. Теория связи в секретных системах / К. Шеннон // Работы по теории информации и кибернетике / К. Шеннон. – М. : ИЛ, 1963. – С. 333 – 402.

9. Романец, Ю. В. Защита информации в компьютерных системах и сетях / Ю. В. Романец, П. А. Тимофеев, В. Ф. Шаньгин ; под ред. В. Ф. Шаньгина. – М. : Радио и связь, 1999. – 328 с.

10. Основы криптографии / А. П. Алферов [и др.]. – М. : Гелиос АРВ, 2001.

11. Бабаш, А. В. Криптография / А. В. Бабаш, Г. П. Шанкин. – М. : СОЛОН-Р, 2002. – 511 с.

Св. план 2009, поз. 44/2

Учебное издание

Виланский Юрий Викторович
Захаров Владимир Владимирович

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Лабораторный практикум
для студентов специальности «Искусственный интеллект»
всех форм обучения

В 2-х частях

Часть 1

Редактор Е. Н. Батурчик
Корректор Л. А. Шичко
Компьютерная верстка Е. С. Чайковская

Подписано в печать	Формат 60x84 1/16.	Бумага офсетная.
Гарнитура «Таймс».	Отпечатано на ризографе.	Усл. печ. л.
Уч.-изд. л. 2,3.	Тираж 100 экз.	Заказ 387.

Издатель и полиграфическое исполнение: учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники»
ЛИ №02330/0494371 от 16.03.2009. ЛП №02330/0494175 от 03.04.2009.
220013, Минск, П. Бровки, 6