МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное общеобразовательное учреждение
высшего профессионального образования
«Курганский государственный университет»

Кафедра «Безопасность информационных и автоматизированных систем»

МАТЕМАТИЧЕСКИЕ ОСНОВЫ КРИПТОГРАФИИ. ТЕОРИЯ СРАВНЕНИЙ И ЕЕ ПРИЛОЖЕНИЯ

Методические указания и контрольные задания
по дисциплине «Криптографические методы защиты информации»
для студентов специальности 090303.65 и направления 231000.62

Курган 2014

Кафедра: «Безопасность информационных и автоматизированных систем»

Дисциплина: «Криптографические методы защиты информации»
(специальность 090303.65, направление 231000.62)

Составил: доц. Т.Р. Змызгова.

Утверждены на заседании кафедры « 29 » января 2014 г.

Рекомендованы методическим советом университета « 14 » февраля 2014 г.

Введение

Большое влияние на развитие криптографии оказали появившиеся в середине 20-го века работы американского математика Клода Шеннона. В этих работах были заложены основы теории информации, а также был разработан математический аппарат для исследований во многих областях науки, снизанных с информацией.

Расширение сфер практического применения криптографии в вопросах защиты информации, появление современных криптографических методов привело к необходимости введения понятий, определений и собственного математического аппарата в этой области.

В силу присущей методам криптографии специфики, большой интерес представляет множество целых чисел и различные алгебраические структуры на его базе. Математические методы, используемые в криптографии, невозможно успешно освоить без знания основ теории чисел и сравнений. Поэтому знание и умение работать с этими понятиями является необходимым условием для подготовки специалистов в области защиты информации.

В методических указаниях рассмотрены основополагающие математические понятия и идеи, необходимые для введения в теорию криптографических алгоритмов и лежащие в основе построения современных криптографических систем, математическим фундаментом которых является прикладная теория чисел.

§1 Основные определения и алгоритмы делимости чисел

Пусть дано множество целых чисел, с элементами которого мы будем работать на протяжении всего курса.

Число ***a делится на b***, если $a=bq$ и $q \in Z$, при этом a называют ***кратным числа*** b, а b – делителем числа a.

Теорема 1 (о делении с остатком). Всякое целое число a можно представить с помощью положительного целого числа b равенством вида $a=bq+r$, $0 \le r > b$.

Число q называется ***неполным частным***, а число r – ***остатком от деления*** a на b.

Всякое целое, делящее одновременно целые a, b называются их ***общим делителем***.

Положительное целое число d является ***наибольшим общим делителем*** чисел a и b, если:

- d является делителем a и b;
- любой делитель a и b является делителем d.

Наибольший из общих делителей чисел a и b обозначается символом (a,b) или $НОД(a,b)$.

Если $НОД(a,b)$, то целые числа a и b называют ***взаимно-простыми***.

Теорема 2 Если $a=bq+c$, то $НОД(a,b)=НОД(b,c)$.

Для отыскания $НОД(a,b)$ при $a > b$ применяется алгоритм Евклида, основанный на теореме 2. Этот алгоритм был изложен в знаменитых книгах Евклида «Начала» в III веке до н.э.

Алгоритм Евклида для вычисления $НОД(a,b)$

1 Вычислим r – остаток от деления числа a на b, $a = bq + r$, $0 \le r < b$.

2 Если $r = 0$, то b – искомое число.

3 Если $r \neq 0$, заменим пару чисел (a,b) парой (b,r) и перейдем к шагу 1.

Общая схема алгоритма Евклида выглядит следующим образом:

$$a = bq_0 + r_1,\ 0 \le r_1 < b,$$
$$b = r_1 q_1 + r_2,\ 0 \le r_2 < r_1,$$
$$r_1 = r_2 q_2 + r_3,\ 0 \le r_3 < r_2,$$
$$\ldots\ldots\ldots\ldots\ldots$$
$$r_{n-2} = r_{n-1} q_{n-1} + r_n,\ 0 \le r_n < r_{n-1},$$
$$r_{n-1} = r_n q_n,$$
$$НОД(a,b) = r_n.$$

Заметим, что на некотором этапе получается остаток, не равный нулю, поэтому процесс деления заканчивается. В противном случае мы имели бы бесконечную убывающую последовательность натуральных чисел $b > r_1 > r_2 > \ldots$, что невозможно. Таким образом, $НОД(a,b)$ равен последнему не равному нулю остатку алгоритма Евклида.

Пример Найти с помощью алгоритма Евклида $НОД(2004,1941)$.

$$2004 = 1941 \cdot 1 + 63,\ 1941 = 63 \cdot 30 + 51,$$
$$53 = 51 \cdot 1 + 12,\ 51 = 12 \cdot 4 + 3,\ 12 = 3 \cdot 4.$$

Итак, $НОД(2004,1941) = 3$.

Пример Найти с помощью алгоритма Евклида $НОД(603,108)$.

$$603 = 5 \cdot 108 + 63,\ 108 = 1 \cdot 63 + 45,$$
$$63 = 1 \cdot 45 + 18,\ 45 = 2 \cdot 18 + 9,$$
$$18 = 2 \cdot 18 + 0.$$

Получаем $НОД(603,108) = 9$.

Замечание При вычислении $НОД(a,b)$ с помощью алгоритма Евклида будет выполнено не более $5p$ операций деления с остатком, где p - количество цифр в десятичной записи меньшего из чисел a и b.

Алгоритм нахождения НОД нескольких чисел $НОД(a_1,a_2,\ldots,a_n)$

Нахождение наибольшего общего делителя трех и большего количества чисел может быть сведено к последовательному нахождению НОД двух чисел:

$$НОД(a_1,a_2) = d_1,\ НОД(d_1,a_3) = d_2,\ НОД(d_2,a_4) = d_3,\ldots,$$
$$НОД(d_{n-2},a_n) = НОД(a_1,a_2,\ldots,a_n) = d_{n-1}.$$

Линейная форма НОД Пусть $НОД(a,b) = d$. Тогда $\exists x, y \in Z$ такие, что $ax + by = d$. Эта запись называется ***линейной формой*** $НОД(a,b)$. Числа x, y называются ***коэффициентами линейной формы***.

Теорема (Соотношение Безу) Если a и b одновременно не равны нулю, то существуют целые числа x, y, называемые ***коэффициентами Безу***, такие что $НОД(a,b) = ax + by$.

Расширенный алгоритм Евклида

С помощью этого алгоритма можно найти не только $НОД(a,b)$, но и линейную форму НОД:

$$r_1 = a - bq_0 = a \cdot 1 + b \cdot (-q_0) = ax_1 + by_1,$$
$$r_2 = b - r_1 q_1 = b - (a - bq_0)q_1 = a \cdot (-q_1) + b \cdot (1 + q_0 q_1) = ax_2 + by_2,$$
$$r_3 = r_1 - r_2 q_2 = a - bq_0 - (a \cdot (-q_1) + b \cdot (1 + q_0 q_1))q_2 =$$
$$= a \cdot (1 + q_1 q_2) + b \cdot (-q_0 - q_2 - q_0 q_1 q_2) = ax_3 + by_3,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$НОД(a,b) = r_n = r_{n-2} - r_{n-1} q_{n-1} = ax_n + by_n.$$

Теорема (Ламе) Вычисление НОД чисел a и b с помощью алгоритма Евклида требует не более $5p$ операций деления с остатком, где p - количество цифр в десятичной записи меньшего из чисел a и b.

Пример С помощью расширенного алгоритма Евклида найти $НОД(a,b)$ и его линейную форму, если $a = 3367$, $b = 1001$.

Результат вычислений приведен в таблице 1. Проследите за вычислениями в последнем столбце таблицы (снизу вверх). На последнем шаге (в верхней строке) получаем выражение, которое позволяет получить линейное представление НОД:

$$91 = 3367 \cdot 3 + 1001 \cdot (-10).$$

Таблица 1 – Прямой и обратный ход расширенного алгоритма Евклида

Первое число	**Второе число**	**Деление нацело**	**Обратный ход алгоритма Евклида**
3367	1001	3367 = **1001**·3+**364**	91 = **(**3367–**1001**·3) ·3–**1001**·1 = = **3367**·3+**1001**·(–10)
364	1001	1001 =**364**·2+**273**	91 = **364**–(1001 – **364**·2) = **364**·3–1001·1
364	273	364 = **273**·1+**91**	91=364–**273**·1
91	273	273 = **91**·3+0	0

Теорема 3 Числа a и b взаимно просты тогда и только тогда, когда существуют целые числа x, y такие, что $ax + by = 1$.

§ 2 Простые числа

Простым числом p называется целое число, которое не имеет никаких делителей кроме 1 и самого себя.

Число 1 (единица) рассматривается особо, оно не является ни простым, ни составным.

В 1876 г. Француз Люка доказал, что число $(2^{127}-1)$ – простое и 75 лет оно оставалось наибольшим из известных простых чисел.

В настоящее время составлены таблицы всех простых чисел, не превосходящих 50 млн. Существует бесконечно много простых чисел. В криптографии, особенно в криптографии с открытыми ключами используют большие простые числа порядка 512 бит и более.

Один из самых старых и известных алгоритмов проверки простоты числа – проверка делением: если число $n>1$ не делится ни на одно простое число меньшее или равное $\sqrt{n}$, то n – простое число.

Основная теорема арифметики (теорема факторизации) Всякое целое число, отличное от -1, 0 и 1, единственным образом (с точностью до порядка сомножителей) разложимо в произведение простых чисел.

Каноническое разложение Любое целое положительное число *n* может быть представлено в канонической форме, т.е. в виде произведения некоторых простых чисел в соответствующих степенях, а именно:

$$n = p_1^{n_1} p_2^{n_2} ... p_k^{n_k},$$

где $p_1, p_2, ..., p_k$ – простые числа, $n_1, n_2, ..., n_k$ – целые положительные числа.

Функция Эйлера $\varphi(n)$ – это количество положительных целых чисел, меньших *n* и взаимно простых с n.

Очевидно, что $\varphi(6)=2$, так как из чисел 1, 2, 3, 4, 5 только 1 и 5 являются взаимно простыми с числом 6.

Пусть $n = p_1^{n_1} p_2^{n_2} ... p_k^{n_k}$ – каноническое разложение числа *n*, тогда справедлива ***формула Эйлера***:

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

В частности,

$$\varphi(p) = p-1,\ \varphi(p^{\alpha}) = p^{\alpha-1}(p-1).$$

Очевидно, что если $n = pq$, где *p* и *q* – простые числа, т.е. $НОД(p,q)=1$, то

$$\varphi(n) = \varphi(p)\varphi(q) \text{ или } \varphi(n) = (p-1)(q-1).$$

Пример Вычислим значение функции Эйлера $\varphi(1001)$.

Очевидно, что $1001 = 7\cdot 11\cdot 13$. Тогда

$$\varphi(1001) = \varphi(7)\cdot\varphi(11)\cdot\varphi(13) = (7-1)(11-1)(13-1) = 720.$$

Каноническое разложение чисел *a* и *b* можно использовать для нахождения $НОД(a,b)$.

Теорема Пусть каноническое разложение натуральных чисел *a* и *b* имеет вид:

$$a = p_1^{\alpha_1} p_2^{\alpha_2} ... p_m^{\alpha_m},\ b = p_1^{\beta_1} p_2^{\beta_2} ... p_m^{\beta_m},$$

где $\alpha_i \ge 0, \beta_i \ge 0$. Тогда

$$НОД(a,b) = p_1^{\min(\alpha,\beta_1)} p_2^{\min(\alpha_2,\beta_2)} ... p_m^{\min(\alpha_m,\beta_m)}.$$

Замечание 1 Если простое число p_i входит в одно из разложений, а в другое – нет, то дополнительный сомножитель p_i следует вставить в нулевой степени в то разложение, где его нет.

Замечание 2 Очевидно, что НОД нескольких чисел произведению степеней вида p^{α}, где p – простой делитель всех этих чисел, α – наименьший из показателей, с которыми p входит в их канонические разложения.

Пример Пусть $a = 1200500$, $b = 72342816$. Имеем

$$a = 2^2 \cdot 5^3 \cdot 7^4,\ b = 2^5 \cdot 3^1 \cdot 7^3 \cdot 13^3$$

или

$$a = 2^2 \cdot 3^0 \cdot 5^3 \cdot 7^4 \cdot 13^0,\ b = 2^5 \cdot 3^1 \cdot 5^0 \cdot 7^3 \cdot 13^3.$$

Тогда $НОД(a,b) = 2^2 \cdot 3^0 \cdot 5^0 \cdot 7^3 \cdot 13^0 = 2^2 \cdot 7^3 = 1372$.

§ 3 Теория сравнений

Если a является целым, а z – положительным целым числом, то $a \bmod z$ определяется как остаток от деления a на z. Тогда для любого целого числа a можно написать $a = [a/z] \cdot z + (a \bmod z)$, где $[a/z]$ – наибольшее целое число, не превышающее a/z.

Пример Очевидно, что $11 \bmod 7 = 4$, так как $11 = [11/7] \cdot 7 + 4 = 1 \cdot 7 + 4$.

Два целых числа a и b называются ***сравнимыми по модулю*** m, если

$$a \bmod m = b \bmod m \text{ или } a \equiv b (\bmod m).$$

Пример $73 \equiv 4 (\bmod 23)$, так как остатки от деления чисел 73 и 4 на 23 совпадают.

Можно утверждать, что целые числа a и b являются ***сравнимыми по модулю*** m, если выполняется одно из утверждений:

1 $(a-b) \vdots m$;

2 $\exists q_1, q_2$, что $a = mq_1 + r$, $b = mq_2 + r$;

3 $\exists q$, что $a = mq + b$.

Иногда число b называют ***вычетом*** a по модулю m. Операция $a \bmod m$ называется ***приведением по модулю***, она эквивалентна отысканию вычета a по модулю m (остатка от деления a на модуль m).

Пример

1 $8 \equiv 5 (\bmod 3)$, так как $8-5=3$ и $3 \vdots 3$.

2 $12 \equiv 2 (\bmod 5)$, так как $12-2=10$ и $10 \vdots 5$.

3 $3 \equiv 7 (\bmod 2)$, так как $3-7=-4$ и $-4 \vdots 2$.

4 $11 \neq 3 (\bmod 5)$, так как $11-3=8$ и $8 \not\vdots 5$.

Свойства сравнений

Теорема 1 Имеют место следующие утверждения:

1) если $a \equiv b (\bmod m)$ и $k \in Z$, то $k \cdot a \equiv k \cdot b (\bmod m)$;

2) если $k \cdot a \equiv k \cdot b (\bmod m)$ и числа k, m взаимнопросты, то $a \equiv b (\bmod m)$;

3) если $a \equiv b(\mathrm{mod}\, m)$ и $k \in N$, то $k \cdot a \equiv k \cdot b(\mathrm{mod}\, k \cdot m)$;

4) если $k \cdot a \equiv k \cdot b(\mathrm{mod}\, k \cdot m)$ и $k, m \in N$, то $a \equiv b(\mathrm{mod}\, m)$;

5) если $a \equiv b(\mathrm{mod}\, m)$ и $c \equiv d(\mathrm{mod}\, m)$, то $a + c \equiv b + d(\mathrm{mod}\, m)$;

6) если $a \equiv b(\mathrm{mod}\, m)$ и $c \equiv d(\mathrm{mod}\, m)$, то $a \cdot c \equiv b \cdot d(\mathrm{mod}\, m)$;

7) если $a \equiv b(\mathrm{mod}\, m)$ и $n \in N$, то $a^n \equiv b^n(\mathrm{mod}\, m)$.

Теорема 2 Любое слагаемое в левой или правой части сравнения можно перенести в другую часть с противоположным знаком, т.е. если $a + b \equiv c(\mathrm{mod}\, m)$, то $a \equiv c - b(\mathrm{mod}\, m)$.

Теорема 3 В сравнениях по модулю m можно отбрасывать или добавлять слагаемые, делящиеся на число m, т.е., если, например, $c \vdots m$ и $a \equiv b(\mathrm{mod}\, m)$, то $a \pm c \equiv b(\mathrm{mod}\, m)$ или $a \equiv b \pm c(\mathrm{mod}\, m)$.

Для однозначности операции приведения по модулю, как правило, ***рассматривают положительные вычеты***.

Множество чисел от *0* до $m-1$ называют ***полной системой вычетов по модулю m***. Это означает, что для любого целого числа *a* его остаток от деления (вычет) на модуль *m* является некоторым числом из этой системы.

Арифметика остатков

- $(a \pm b) \bmod m = ((a \bmod m) \pm (b \bmod m)) \bmod m$;
- $(a \cdot b) \bmod m = ((a \bmod m) \cdot (b \bmod m)) \bmod m$;
- $(a + b)c \bmod m = ((ac \bmod m) + (bc \bmod m)) \bmod m$.

Пример

$$(341 \cdot 1258) \bmod 3 = ((341 \bmod 3) \cdot (1258 \bmod 3)) \bmod 3 = 2 \cdot 1 \bmod 3 = 2.$$

Малая теорема Ферма Для любого простого *p* и любого $a \geq 1$, не делящегося на *p*, справедливо сравнение

$$a^{p-1} \equiv 1(\mathrm{mod}\, p).$$

Теорема Эйлера Для любого модуля *m* и любого $a \geq 1$, взаимно простого с *m*, справедливо сравнение

$$a^{\varphi(m)} \equiv 1(\mathrm{mod}\, m).$$

Решение сравнений 1-й степени методом Эйлера

Пусть задано сравнение

$$ax \equiv b(\mathrm{mod}\, m), \text{ где } НОД(a, m) = 1.$$

По теореме Эйлера

$$a^{\varphi(m)} \equiv 1(\mathrm{mod}\, m) \text{ или } a(a^{\varphi(m)-1} b) \equiv b(\mathrm{mod}\, m).$$

Сравнивая это выражение с исходным, получаем

$$x \equiv a^{\varphi(m)-1} b(\mathrm{mod}\, m).$$

Рассмотрим сравнения первой степени:

$$ax \equiv b(\mathrm{mod}\, m).$$

- если $НОД(a, m) = 1$, то сравнение имеет единственное решение $x \equiv a^{\varphi(m)-1} b(\mathrm{mod}\, m)$;
- если $НОД(a, m) = d$ и $d \vdots b$, то сравнение не имеет решений;

- если $НОД(a,m)=d$ и $d \vdots b$, то сравнение имеет d решений.

Пример Решить сравнение $7 \cdot x \equiv 5(\mathrm{mod}\,9)$.

Применим теорему Эйлера:

$$7^{\varphi(9)} \equiv 1(\mathrm{mod}\,9),\ \varphi(9)=6,\ 7^6 \equiv 1(\mathrm{mod}\,9).$$

Умножим обе части сравнения на 7^5:

$$7 \cdot 7^5 \cdot x \equiv 5 \cdot 7^5(\mathrm{mod}\,9),\ 7^6 \cdot x \equiv 5 \cdot 7^5(\mathrm{mod}\,9),\ x \equiv 5 \cdot 7^5(\mathrm{mod}\,9)$$

или

$$x \equiv (-4) \cdot (-2)^5(\mathrm{mod}\,9),\ x \equiv 128(\mathrm{mod}\,9),\ x \equiv 2(\mathrm{mod}\,9).$$

Можно сразу же по общей формуле записать:

$$x \equiv 5 \cdot 7^{\varphi(9)-1}(\mathrm{mod}\,9).$$

Отметим, что метод решения сравнения, основанный на применении теоремы Эйлера, нельзя отнести к рациональным методам решения сравнений.

Очевидно, что сравнение $ax \equiv b(\mathrm{mod}\,m)$ равносильно ***диофантову уравнению*** $ax+my=1$. Так как $НОД(a,m)=1$, то это уравнение можно решить с помощью расширенного алгоритма Евклида.

Пример Решить сравнение $9 \cdot x \equiv 3(\mathrm{mod}\,4)$.

Так как $НОД(a,m)=НОД(9,4)=1$, сравнение имеет единственное решение. Используя свойства сравнений, получаем

$$3 \cdot x \equiv 1(\mathrm{mod}\,4).$$

Это сравнение равносильно уравнению $3x+4y=1$, решая которое с помощью расширенного алгоритма Евклида, получаем $x=-1,\ y=1$.

Таким образом,

$$x \equiv -1(\mathrm{mod}\,4)=3(\mathrm{mod}\,4).$$

Пример Решить уравнение $23 \cdot x+91 \cdot y=2$.

Так как $НОД(23,1)=1$, то уравнение имеет решение в целых числах. Учитывая, что 23 - целое положительное число, его можно принять за модуль соответствующего сравнения, получим

$$91 \cdot y \equiv 2(\mathrm{mod}\,23).$$

Прибавляя к левой части сравнения число $-92 \cdot y$, кратное модулю, приходим к сравнению

$y \equiv -2(\mathrm{mod}\,23)$, т.е. $y=-2+33 \cdot k$, где $k \in Z$.

Подставив полученное значение y в данное уравнение, после простейших преобразований находим, что

$x=8-91 \cdot k$, где $k \in Z$.

Тогда общее решение данного уравнения можно записать в виде:

$x=8-91 \cdot k,\ y=-2-23 \cdot k$, где $k \in Z$.

Вычисление степени некоторого числа по модулю

Непосредственное вычисление выражения $a^n \bmod m$ представляет собой простую последовательность умножений и делений, но такой способ не- при-

емлем для больших степеней. Существуют специальные приемы, ускоряющие эту операцию, минимизируя количество умножений по модулю.

а) алгоритм быстрого возведения в степень по модулю

Пусть требуется вычислить $a^n \bmod m$.

1 Представим число n в двоичной системе счисления: $n_{10} = (b_1 b_2 ... b_k)_2$, где $b_i \in \{0,1\}$.

2 Заполним следующую таблицу:

b	b_0	b_1	…	b_k
a	a_0	a_1	…	a_k

Здесь

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

Тогда искомый результат появится в последней ячейке второй строки таблицы.

Пример Вычислить $5^{29} \bmod 7$.

Имеем $29_{10} = 11101_2$. Заполним таблицу согласно приведенному алгоритму:

b	1	1	1	0	1
a	5	6	5	4	3

Здесь

$$a_0 = a = 5,\ a_1 = a_0^2 \cdot a \bmod 7 = 25 \cdot 5 \bmod 7 = 6,$$
$$a_2 = a_1^2 \cdot a \bmod 7 = 36 \cdot 5 \bmod 7 = 5,\ a_3 = a_2^2 \bmod 7 = 25 \bmod 7 = 4,$$
$$a_4 = a_3^2 \cdot a \bmod 7 = 16 \cdot 5 \bmod 7 = 3.$$

Тогда $5^{29} \bmod 7 = 3$.

Пример Вычислить $2^{199} \bmod 1003$.

Имеем $199_{10} = 11000111_2$. Заполним таблицу согласно вышеприведенному алгоритму:

b	1	1	0	0	0	1	1	1
a	2	8	64	84	35	444	93	247

Тогда

$$2^{199} \bmod 1003 = 247.$$

Можно представить этот алгоритм иначе:

1) запишем число n в двоичной системе счисления:

$$n = b_0 2^r + ... + b_{r-1} 2 + b_k,$$

где b_i, $i = \overline{1,k}$, – цифры в двоичном представлении, равные 0 или 1, $n_0 = 1$.

2) положим $a_0 = a$ и затем для $i = \overline{1,k}$ вычислим

$$a_i = a_{i-1}^2 \cdot a^{b_i} \pmod m.$$

3) a_r – искомый вычет $a^n \bmod m$.

б) цепочка сложений

Можно произвести возведение в степень как ряд последовательных умножений, выполняя каждый раз приведение по модулю:

$$a^{2^n} \pmod m = \underbrace{\left(\left(\left(a^2 \bmod m\right)^2 \bmod m\right)^2 \bmod m\right)^2 \ldots \bmod m}_{n} \bmod m.$$

Если показатель не является степенью 2, то его нужно представить в виде произведения степеней с показателями, являющимися степенями 2:

$$a^n \pmod m = a^{2^{n_1}} \cdot a^{2^{n_2}} \ldots a^{2^{n_k}} \pmod m, \text{ где } n_1 + n_2 + \ldots + n_k = n.$$

Пример

$$5^{29} \bmod 7 = \left(5^{16} \cdot 5^8 \cdot 5^4 \cdot 5\right) \bmod 7 = \left(\left(\left(5^2\right)^2\right)^2\right)^2 \cdot \left(\left(5^2\right)^2\right)^2 \cdot \left(5^2\right)^2 \cdot 5 \bmod 7 =$$

$$= \left(\left(\left(5^2\right)^2\right)^2 \cdot \left(5^2\right)^2 \cdot 5^2\right)^2 \cdot 5 \bmod 7 = \left(\left(\left(5^2\right)^2 \cdot 5^2 \cdot 5\right)^2\right)^2 \cdot 5 \bmod 7 = \left(\left(\left(5^2 \cdot 5\right)^2 \cdot 5\right)^2\right)^2 \cdot 5 \bmod 7 =$$

$$= \left(\left(\left(\left(\left(5^2 \bmod 7\right) \cdot 5 \bmod 7\right)^2 \bmod 7\right) \cdot 5 \bmod 7\right)^2 \bmod 7\right)^2 \bmod 7 \cdot 5\Big) \bmod 7 =$$

$$= 2 \cdot 5 \bmod 7 = 3 \bmod 7.$$

в) понижение показателя при помощи теоремы Эйлера

Пусть $НОД(a,m) = 1$ и $n > \varphi(m)$. Тогда имеет место равенство

$$n = \varphi(m)q + r.$$

Отсюда

$$a^n \bmod m = a^{\varphi(m)q+r} \bmod m = a^{\varphi(m)q} a^r \bmod m = a^r \bmod m.$$

Пример Вычислить $5^{29} \bmod 7$.

Имеем $n = 29$, $m = 7, a = 5$, причем $\varphi(7) = 6$, $НОД(a,m) = 1$. Тогда

$$n = 29 = \varphi(m)q + r = 6 \cdot 4 + 5, \text{ т.е. } r = 5.$$

Отсюда

$$5^{29} \bmod 7 = 5^{6 \cdot 4 + 5} \bmod 7 = 5^5 \bmod 7 = \left(\left(5^2\right)^2 \cdot 5\right) \bmod 7 =$$

$$= \left(\left(5^2 \bmod 7\right)^2 \bmod 7 \cdot 5\right) \bmod 7 = \left(4^2 \bmod 7 \cdot 5\right) \bmod 7 =$$

$$2 \cdot 5 \bmod 7 = 3.$$

Пример Найти остаток от деления числа 3^{28} на 7.

Так как $3^6 \equiv 1 (\bmod 7)$, то

$$3^{28} \equiv 3^{6 \cdot 4 + 4} \equiv \left(3^6\right)^4 \cdot 3^4 \equiv 3^4 \equiv 81 \equiv 4 (\bmod 7).$$

Очевидно, что искомый остаток равен 4.

Пример Найти остаток от деления 243^{132} на 34.

Имеем $243 \equiv 5 (\bmod 34)$. Так как $НОД(5,34) = 1$, то согласно теореме Эйлера

$$5^{\varphi(34)} \equiv 1 (\bmod 34) \text{ или } 5^{16} \equiv 1 (\bmod 34).$$

Тогда

$$243^{132} \equiv 5^{132} \equiv 5^{16 \cdot 8 + 4} = (5^{16})^8 \cdot 5^4 \equiv 1^8 \cdot 625 \equiv 13 (\bmod 34).$$

Следовательно, искомый остаток равен 13.

Пример Вычислить последние две цифры числа 1988^{1988}.

Последние две цифры числа образуют остаток при делении этого числа на 100, т.е.

$$1988^{1988} \equiv x(\mathrm{mod}100), \text{ где } 0 \le x < 100.$$

Так как

$$1988 \equiv 88 \equiv -12(\mathrm{mod}100),$$

то

$$x \equiv 12^{1988}(\mathrm{mod}100).$$

Очевидно, что $НОД(12,100) = 4,$ поэтому теорему Эйлера применить нельзя. Положим $x = 4 \cdot y$, имеем

$$4 \cdot y \equiv 12 \cdot 12^{1987}(\mathrm{mod}\, 4 \cdot 25).$$

Отсюда

$$y = 3 \cdot 12^{1987}(\mathrm{mod}\, 25).$$

Применяем теорему Эйлера:

$$(12,25) = 1,\ 12^{\varphi(25)} \equiv 1(\mathrm{mod}\, 25),$$
$$\varphi(25) = 20,\ 12^{20} \equiv 1(\mathrm{mod}\, 25).$$

Тогда

$$y = 3 \cdot (12^{20})^{99} \cdot 12^{7} \equiv 3 \cdot 12^{7}(\mathrm{mod}\, 25).$$

Так как

$$12^{2} \equiv 144 \equiv -6(\mathrm{mod}\, 25),$$

то

$$12^{4} \equiv (-6)^{2} \equiv 11(\mathrm{mod}\, 25),\ y \equiv 3 \cdot 12^{2} \cdot 12^{4} \cdot 12 \equiv 3 \cdot (-6) \cdot 11 \cdot 12 \equiv 24(\mathrm{mod}\, 25).$$

Значит, $x \equiv 96(\mathrm{mod}100)$, т.е. 9 и 6 - последние две цифры числа 1988^{1988}.

Пример. Девятая степень однозначного числа n оканчивается цифрой 7; найти это число.

Так как девятая степень числа n оканчивается цифрой 7, то остаток от деления n^9 на 10 должен быть равен 7, т.е. справедливо сравнение:

$$n^{9} \equiv 7(\mathrm{mod}10).$$

Так как $НОД(7,10) = 1$, то $НОД(n,10) = 1$. Воспользовавшись теоремой Эйлера, получим

$$n^{\varphi(10)} \equiv 1(\mathrm{mod}10),\ n^{4} \equiv 1(\mathrm{mod}10) \text{ или } n^{8} \equiv 1(\mathrm{mod}10).$$

Тогда сравнение $n^{9} \equiv 7(\mathrm{mod}10)$ примет вид:

$$n \equiv 7(\mathrm{mod}10).$$

Так как по условию n определяется однозначно, выбираем наименьший положительный вычет, т.е. $n = 7$.

§4 Системы сравнений

Одним из важных результатов теории чисел является так называемая китайская теорема об остатках. По существу эта теорема утверждает, что можно восстановить целое число по множеству его остатков от деления на числа из

некоторого набора попарно взаимно простых чисел. Эта теорема была описана в трактате китайского математика Сунь Цзы, предположительно датируемом III веком н.э.

Китайская теорема об остатках. Если числа $a_1, a_2, ..., a_n$ попарно взаимно просты, то для любых остатков $r_1, r_2, ..., r_n$ таких, что $0 \le r_i < a_i$, $i = \overline{1,n}$, найдётся число N, которое при делении на a_i, даёт остаток r_i при всех $i = \overline{1,n}$.

Рассмотрим систему сравнений следующего вида:

$$\begin{cases} x \equiv a_1 (\mathrm{mod}\, m_1), \\ x \equiv a_2 (\mathrm{mod}\, m_2), \\ ..... \\ x \equiv a_k (\mathrm{mod}\, m_k), \end{cases}$$

Если модули $m_1, m_2, ..., m_k$ попарно взаимно просты, система совместна и имеет единственное решение.

Обозначим $M = m_1 \cdot m_2 \cdot ... \cdot m_k$ и выберем $y_1, y_2, ..., y_k$ так, что

$$\begin{cases} M_1 y_1 \equiv 1 (\mathrm{mod}\, m_1), \\ M_2 y_2 \equiv 1 (\mathrm{mod}\, m_2), \\ .... \\ M_k y_k \equiv 1 (\mathrm{mod}\, m_k), \end{cases}$$

где $M_i = \dfrac{M}{m_i}$, $i = \overline{1,k}$.

Тогда решение системы будет иметь вид:

$$x \,\mathrm{mod}\, M = M_1 y_1 a_1 + M_2 y_2 a_2 + ... + M_k y_k a_k .$$

Пример. Решить систему сравнений

$$\begin{cases} x \equiv 7 (\mathrm{mod}\, 8), \\ x \equiv -1 (\mathrm{mod}\, 11), \\ x \equiv 3 (\mathrm{mod}\, 15). \end{cases}$$

Очевидно, что модули $m_1 = 8, m_2 = 11, m_3 = 15$ попарно взаимно просты, т.е. данная система совместна и имеет единственное решение.

Вычисляем

$$M = m_1 m_2 m_3 = 8 \cdot 11 \cdot 15 = 1320.$$

Тогда

$$M_1 = \frac{M}{m_1} = \frac{1320}{8} = 165,\ M_2 = \frac{M}{m_2} = \frac{1320}{11} = 120,\ M_3 = \frac{M}{m_3} = \frac{1320}{15} = 88.$$

Рассмотрим вспомогательную систему сравнений:

$$\begin{cases} M_1 y_1 \equiv 1 (\mathrm{mod}\, m_1), \\ M_2 y_2 \equiv 1 (\mathrm{mod}\, m_2), \\ M_3 y_3 \equiv 1 (\mathrm{mod}\, m_3) \end{cases} \text{ или } \begin{cases} 165 y_1 \equiv 1 (\mathrm{mod}\, 8), \\ 120 y_2 \equiv 1 (\mathrm{mod}\, 11), \\ 88 y_3 \equiv 1 (\mathrm{mod}\, 15). \end{cases}$$

Очевидно, что последняя система эквивалентна следующей:

$$\begin{cases} 5y_1 \equiv 1 (\mathrm{mod}\, 8), \\ 10y_2 \equiv 1 (\mathrm{mod}\, 11), \\ 13y_3 \equiv 1 (\mathrm{mod}\, 15). \end{cases}$$

Находим

$$y_1 = 5,\ y_2 = 10,\ y_3 = 7.$$

Получаем

$$x \equiv 165 \cdot 5 \cdot 7 + 120 \cdot 10 \cdot (-1) + 88 \cdot 7 \cdot 3 (\mathrm{mod}\, 1320) \equiv 1143 (\mathrm{mod}\, 1320).$$

§ 5 Квадратичные вычеты. Символы Лежандра и Якоби

Рассмотрим сравнение

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

где p - простое число, причем $НОД(a, p) = 1, 1 \le a < p,\ p > 2$.

Число a называется ***квадратичным вычетом*** по простому модулю p, если данное сравнение разрешимо, т.е. имеет решение, и называют ***квадратичным невычетом*** по этому модулю, если сравнение неразрешимо.

Если a - квадратичный вычет по модулю p, полученный возведением в квадрат числа x, то это же число будет получено возведением в квадрат числа $-x \equiv p - x (\mathrm{mod}\, p)$. Поэтому все квадратичные вычеты по модулю p можно найти возведением в квадрат чисел 1, 2, 3,...,(p–1)/2. Таким образом, для любого нечетного числа p имеется ровно (p–1)/2 квадратичных вычетов и столько же квадратичных невычетов.

Если $n = pq$, где p и q - простые числа, то существует $\frac{(p-1)(q-1)}{4}$ квадратичных вычетов по модулю n.

Пример Очевидно, что число 2 является квадратичным вычетом по модулю 7, так как $4^2 = 16 \equiv 2 (\mathrm{mod}\, 7)$.

Заметим, что сравнение $x^2 \equiv 2 (\mathrm{mod}\, 7)$ имеет еще и другое решение $3^2 = 9 \equiv 2 (\mathrm{mod}\, 7)$. Число 3 является квадратичным невычетом по модулю 7, так как сравнение $x^2 \equiv 3 (\mathrm{mod}\, 7)$ решений не имеет. В этом можно убедиться последовательным перебором полной системы вычетов $x = \{0,1,2,3,4,5,6\}$.

Пример. Найдем все квадратичные вычеты и невычеты по модулю $p = 17$.

Количество вычетов определяем по формуле:

$$\frac{p-1}{4} = \frac{17-1}{2} = 8.$$

Легко проверить, что

$$1^2 \equiv 1 (\mathrm{mod}\, 17),\ 2^2 \equiv 4 (\mathrm{mod}\, 17),\ 3^2 \equiv 9 (\mathrm{mod}\, 17),\ 4^2 \equiv 16 (\mathrm{mod}\, 17),$$
$$5^2 \equiv 8 (\mathrm{mod}\, 17),\ 6^2 \equiv 2 (\mathrm{mod}\, 17),\ 7^2 \equiv 15 (\mathrm{mod}\, 17),\ 8^2 \equiv 13 (\mathrm{mod}\, 17),$$
$$9^2 \equiv 13 (\mathrm{mod}\, 17),\ 10^2 \equiv 15 (\mathrm{mod}\, 17),\ 11^2 \equiv 2 (\mathrm{mod}\, 17),\ 12^2 \equiv 8 (\mathrm{mod}\, 17),$$
$$13^2 \equiv 16 (\mathrm{mod}\, 17),\ 14^2 \equiv 9 (\mathrm{mod}\, 17),\ 15^2 \equiv 4 (\mathrm{mod}\, 17),\ 16^2 \equiv 1 (\mathrm{mod}\, 17).$$

Отсюда видно, что числа 1, 2, 4, 8, 9, 13, 15, 16 являются квадратичными вычетами по модулю 17, а 3, 5, 6, 7, 10, 11, 12, 14 являются квадратичными невычетами по модулю 17.

Символ Лежандра $\left(\frac{a}{p}\right)$ определяется для всех целых чисел a, которые не делятся на простое число $p>2$, равенством:

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

Иногда символ Лежандра дополняют для чисел $a \vdots p$, полагая $\left(\frac{a}{p}\right)=0$. Используется и иное обозначение $L(a,p)$.

При помощи критерия Эйлера, можно показать, что

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

Свойства символа Лежандра:

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

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

3) $\left(\frac{1}{p}\right)=1$;

4) $\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$;

5) $\left(\frac{a_1a_2\ldots a_k}{p}\right)=\left(\frac{a_1}{p}\right)\cdot\left(\frac{a_2}{p}\right)\cdot\ldots\cdot\left(\frac{a_k}{p}\right)$;

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

7) Закон взаимности квадратичных вычетов для простых, нечетных q, p:

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

Следствие:

1) $\left(\frac{ab^2}{p}\right)=\left(\frac{a}{p}\right)$ для всех b, $НОД(a,p)=1$;

2) $\left(\frac{a^k}{p}\right)=\left(\frac{a}{p}\right)^k$;

3) если $a=p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_m^{\alpha_m}$, то

$$\left(\frac{p_1^{n_1}\cdot p_2^{n_2}\cdot\ldots\cdot p_k^{n_k}}{p}\right)=\left(\frac{p_1}{p}\right)^{n_1}\cdot\left(\frac{p_2}{p}\right)^{n_2}\cdot\ldots\cdot\left(\frac{p_k}{p}\right)^{n_k}.$$

Обобщением символа Лежандра является ***символ Якоби*** для любого числа a и составного нечетного модуля m.

Пусть $m>1$ – нечетное число и $m=p_1\cdot p_2\cdot\ldots\cdot p_k$ – его каноническое разложение его на простые множители, среди которых могут быть и равные.

Если $НОД(a,m)=1$, то символ Якоби $J(a,m)$ определяется равенством:

$$J(a,m)=\left(\frac{a}{p_1}\right)\cdot\left(\frac{a}{p_2}\right)\cdot\ldots\cdot\left(\frac{a}{p_k}\right).$$

Известные свойства символа Лежандра дают возможность установить аналогичные свойства и для символа Якоби.

Свойства символа Якоби:

1) $J(a,m)=0\Leftrightarrow НОД(a,m)\neq 1$;

2) $J(ab,m)=J(a,m)J(b,m)$;

3) $J(a,mn)=J(a,m)J(a,n)$, где $НОД(a,mn)=1$, m,n – нечетные натуральные числа;

4) $a\equiv b(\mathrm{mod}\,p)\Rightarrow J(a,n)J(b,n)$;

5) $J(1,m)=1$;

6) $J(-1,m)=(-1)^{\frac{m-1}{2}}$;

7) $J(2,m)=(-1)^{\frac{m^2-1}{8}}$;

8) $J(m,n)=(-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}J(n,m)$, где $НОД(a,mn)=1$, m,n - нечетные натуральные числа.

Пример Вычислить символ Лежандра $\left(\frac{47}{73}\right)$.

Применяя свойства Лежандра и закон взаимности, находим

$$\left(\frac{47}{73}\right)=(-1)^{23\cdot 36}\cdot\left(\frac{73}{47}\right)=\left(\frac{26}{47}\right)=\left(\frac{2}{47}\right)\cdot\left(\frac{13}{47}\right)=(-1)^{\frac{47^2-1}{8}}\cdot(-1)^{6\cdot 23}\cdot\left(\frac{47}{13}\right)=$$

$$=\left(\frac{8}{13}\right)=\left(\frac{2^2}{13}\right)\cdot\left(\frac{2}{13}\right)=(-1)^{\frac{13^2-1}{8}}=-1.$$

Пример Вычислить символ Якоби $J(131,255)$.

Очевидно, что $255=3\cdot 5\cdot 17$. Имеем

$$J(131,255)=J(131,3)J(131,5)J(131,17).$$

Вычислим каждый сомножитель отдельно:

$$J(131,3)=\left(\frac{2}{3}\right)=(-1)^{\frac{3^2-1}{8}}=-1,\ J(131,5)=\left(\frac{1}{5}\right)=1,$$

$$J(131,17)=\left(\frac{12}{17}\right)=\left(\frac{2}{17}\right)^2\left(\frac{3}{17}\right)=\left(\frac{3}{17}\right)=\left(\frac{17}{3}\right)\cdot(-1)^{\frac{17-1}{2}\cdot\frac{3-1}{2}}=$$

$$=\left(\frac{17}{3}\right)=\left(\frac{2}{3}\right)=-1.$$

Итак,

$$J(131,255) = J(131,3)J(131,5)J(131,17) = (-1)\cdot 1\cdot(-1) = 1.$$

§ 6 Тестирование чисел на простоту

Задачи проверки простоты натурального числа и построения больших простых чисел имеют важные приложения в криптографии. Пусть $n \in N$. Как проверить, является ли число *n* простым?

Существует две группы алгоритмов проверки на простоту: детерминированные и вероятностные.

Детерминированный алгоритм всегда действует по одной и той же схеме и гарантированно решает поставленную задачу (или не дает никакого ответа).

Вероятностный алгоритм использует генератор случайных чисел и дает не гарантированно точный ответ. Вероятностные алгоритмы в общем случае не менее эффективны, чем детерминированные. Если используемый генератор случайных чисел всегда дает набор одних и тех чисел, зависящих от входных данных, то вероятностный алгоритм становится детерминированным.

1 Детерминированные алгоритмы проверки простоты чисел

1) Решето Эратосфена

Одной из самых больших загадок математики является расположение и количество простых чисел в ряду всех натуральных чисел. В этих подсчетах весьма полезным оказался метод, восходящий еще к древнегреческому ученому Эратосфену (III век до н.э). Он придумал для этого алгоритм, известный, как «решето Эратосфена».

Начнем с простого числа 2. Будем выбрасывать каждое второе число, начиная с 2 (кроме самого числа 2), т.е. чётные числа 4, 6, 8, 10 и т.д., подчеркивая каждое из них. После этой операции первым неподчёркнутым числом будет число 3. Оно простое, так как не делится на 2. Оставив число 3 неподчёркнутым, будем подчеркивать каждое третье число после него, т.е. числа 6, 9, 12, 15…; некоторые из них уже были подчеркнуты, поскольку они являются чётными. На следующем шаге первым неподчёркнутым числом окажется число 5; оно простое, так как не делится ни на 2, ни на 3. Оставим число 5 неподчёркнутым, но подчеркнем каждое пятое число после него, т.е. числа 10, 15, 20, 25…; как и раньше, часть из них уже оказалась подчёркнутой. Теперь наименьшим неподчёркнутым числом окажется число 7. Оно простое, так как не делится ни на одно из меньших его простых чисел 2, 3, 5. Повторяя этот процесс, мы получим последовательность неподчёркнутых чисел; все они (кроме числа 1) являются простыми.

Так как во времена Эратосфена писали на восковых табличках и не вычеркивали, а «выкалывали» цифры, то табличка после описанного процесса напоминала решето. Поэтому метод Эратосфена для нахождения простых чисел получил название «решето Эратосфена».

Алгоритм:

1 Создать список последовательных натуральных чисел от 2 до *n*.

2 Пусть – первое простое число.

3 Зачеркнуть все последующие числа в списке с разницей в *p*, т.е. *2p, 3p, 4p* и т.д. В случае $p = 2$ это будут числа *4, 6, 8* и т.д.

4 Поменять значение *p* на первое не зачеркнутое число после *p*.

5 Повторить шаги 3-4 пока $p^2 < n$.

6 Все оставшиеся не зачеркнутыми числа - простые.

2) Метод пробных делений

Разделим число $n \in N$ последовательно на числа $2, 3, \ldots, \sqrt{n}$. Если при каком-нибудь делении мы получим нулевой остаток, то число n – составное, а делитель и частное являются его сомножителями. В противном случае, число n – простое.

Каково время работы этого теста? Очевидно, необходимо выполнить $\sqrt{n}$ делений, поэтому время проверки простоты данного числа равно $O(\sqrt{n})$. Эта оценка не является полиномиальной, поскольку, если учитывать длину $L(n)$ записи n, она принимает вид $O(2^{L(m)/2})$. Таким образом, это экспоненциальный тест, т.е. он очень медленный. Поэтому уже для чисел порядка $10^{30} - 10^{40}$ он не применим. Заметим, что данный тест, кроме проверки на простоту, находит и сомножители составного числа.

3) Метод Вильсона

Теорема Вильсона Выражение

$$(n-1)! \equiv -1 (\mathrm{mod}\, n)$$

справедливо тогда и только тогда, когда *n* – простое.

Замечание Необходимость использования факториала $(n-1)!$ является большим недостатком этого теста, поскольку метод, известный, как «решето Эратосфена», оказывается очень быстрым по сравнению с проверкой делимости числа $(n-1)!+1$ для больших значений *n*. Если *n* имеет 100 цифр, то $(n-1)!$ состоит примерно из 100^{102} цифр.

4) Метод Лукаса

Тест Лукаса Пусть *n* – простое число. Тогда существует натуральное число b, $b < n$, порядок которого по модулю n равен $n-1$, т.е.

$$b^{n-1} \equiv 1 (\mathrm{mod} n),$$

причем никакая меньшая степень числа b не сравнима с $1(\mathrm{mod} n)$.

Следующая теорема является обратным утверждением.

Теорема Пусть *n* – целое число, $n \geq 2$. Если существует число b, $b < n$, такое, что порядок b по модулю n равен $n-1$, т.е.

$$b \equiv (n-1) (\mathrm{mod} n),$$

то *n* – простое число.

2 Вероятностные алгоритмы проверки простоты чисел

Все приведенные выше тесты являются детерминистическими, т.е. для заданного числа *n* мы всегда получаем ответ, является ли оно простым или составным. Если заменить слово «всегда» на выражение «с некоторой вероятностью», то оказывается возможным построить ***вероятностные тесты*** на про-

стоту, которые работают за полиномиальное время. Такие тесты называют ***тестами «псевдопростоты»***.

Пусть $n \in N$, n – нечетное, $n > 1$. Вероятностный тест на простоту проводится следующим образом. Выбирается случайное значение $a \in N$, $1 < a < n$, и для него проверяется выполнение некоторых условий. Если какое-то из условий не выполнено, то число n – составное, поскольку для простых чисел эти условия являются необходимыми. Если же все условия выполнены, то из этого еще не следует простота n. Однако можно будет считать, что «n – простое число с некоторой вероятностью». Кроме того, обычно доказывают оценку снизу для этой вероятности. Чем больше значений a мы протестируем, тем ближе эта вероятность к единице.

Более точно, под тестом «псевдопростоты» мы будем понимать тест, применяемый к паре целых чисел (a,n), обладающий следующими свойствами:

1) тест может выдавать следующие ответы: «n – составное число» или «ответ не удалось определить»;

2) если тест выдал ответ «n - составное число», то n – составное;

3) время выполнения теста полиномиально зависит от $L(n)$ – числа бит в двоичном представлении n.

Для хорошего теста «псевдопростоты» существует фиксированное положительное вещественное число a, такое, что для любого составного числа n тест выдает ответ «составное», по крайней мере, для an выборов различных значений $a \in N$, $1 \le a \le n$.

Кроме того, мы будем говорить, что целое число n является простым с большой вероятностью, если мы подвергли его хорошему тесту псевдопростоты и получили ответ «не удалось определить» для всех оснований a.

1) Первый вероятностный тест

Для заданного значения n выберем случайным образом b, $1 < b < n$. Если $b \mid n$ (b делит n), то тест выдает ответ «n – составное число», в противном случае - «не удалось определить».

Вероятность того, что выдается ответ «n – составное число» равна вероятности того, что $b \mid n$. Если $d(n)$ - число делителей n, а b – случайно выбранное число в пределах $1 < b < n$, то вероятность этого равна $p = |d(n) - 2| / n$.

Очевидно, что это очень слабый тест.

2) Второй вероятностный тест

Для заданного значения n выберем случайным образом b, $1 < b < n$. Если $НОД(b,n) \neq 1$, то тест выдает ответ «n – составное число», в противном случае – «не удалось определить».

Если n – составное число, то количество чисел $b < n$, для которых тест выдает ответ «n – составное число» равно $n - \varphi(n)$. Это количество велико, если n имеет маленькие простые делители. Если $n = pq$, где p, q – большие простые числа, то доля хороших оснований очень мала. Таким образом, этот тест не лучше предыдущего.

3) Тест на основе малой теоремы Ферма

Теорема Если n простое, то для любого целого a выполнено сравнение

$$a^n \equiv a \bmod n .$$

Если этом $НОД(a,n)=1$, то

$$a^{n-1} \equiv 1 \bmod n \qquad (*).$$

Из этой теоремы следует, что если сравнение не выполнено хотя бы для одного числа a, $1 \le a \le n-1$, то n - составное.

Тест является эффективным для обнаружения составных чисел. Можно предложить следующий вероятностный алгоритм:

– выбираем случайное число a, $1 \le a \le n-1$, и проверяем с помощью алгоритма Евклида выполнение условия $НОД(a,n)=1$; если это условие не выполняется, то n - составное;

– если $НОД(a,n) \ne 1$, то проверяем выполнимость сравнения (*); если сравнение не выполняется, то n - составное; если сравнение выполняется, то ответ не известен, т.е. тест выдает ответ «не удалось определить». В этом случае можно повторить тест еще раз.

Если выполняется сравнение (*), то говорят, что число n является ***псевдопростым по основанию a***. Существует бесконечно много пар (a, n), где n - составное и псевдопростое по основанию a.

Этот тест гораздо лучше двух предыдущих, но и он несовершенен, поскольку для всех псевдопростых по основанию b чисел он выдает ответ «не удалось определить».

Пример Очевидно, что

$$2^{341-1} \bmod 341 = 2^{340} \bmod 341 = \left(2^{10}\right)^{34} \bmod 341 = 1024^{34} \bmod 341 = 1 \bmod 341,$$

но $341 = 11 \cdot 31$.

Таким образом, число 341 является псевдопростым по основанию 2.

Из следующей теоремы следует, что существует бесконечно много псевдопростых по основанию 2 чисел.

Теорема Если n - псевдопростое число по основанию 2, то число $2^n - 1$. также является псевдопростым по основанию 2.

Особый случай составляют составные числа n, называемые ***числами Кармайкла***, для которых при всех основаниях $a \in Z$ выполняется сравнение (*).

Минимальные кармайкловы числа - это 561, 1105, 1729, … Множество кармайкловых чисел бесконечно.

Теорема Пусть $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ - представление целого числа n в виде произведения степеней простых чисел. Число n является кармайкловым тогда и только тогда, когда

1) для всякого i показатель степени $\alpha_i = 1$;

2) $k \ge 3$;

3) для всякого i число $p_i - 1$ делит $n-1$.

Пример Покажем, что число 561 является кармайкловым.

Действительно, $561 = 3 \cdot 11 \cdot 17$. Очевидно, что

$$(3-1)\,|\,560,\ (11-1)\,|\,560,\ (17-1)\,|\,560.$$

Число 561 удовлетворяет условиям теоремы, т.е. является кармайкловым.

Таким образом, при применении теста на основе теоремы Ферма может возникнуть три ситуации:

– число n – простое и тест всегда дает ответ «не известно»;

– число n – составное и не является числом Кармайкла, тогда с вероятностью $1/2$ тест дает ответ «n – составное»;

– число n – составное и является числом Кармайкла, тогда тест всегда дает ответ «неизвестно».

Наличие третьей ситуации является очень неудобным свойством данного теста. Для кармайкловых чисел тест простоты, основанный на теореме Ферма, не работает. Тем не менее, его модификация, предложенная Рабином, применима к любым целым числам.

4) Тест Рабина-Миллера

Теорема 1 Пусть n – нечетное составное число, $n-1=2^r t$, где t – нечетно. Тогда количество целых чисел a, $0\le a\le n-1$, удовлетворяющих условиям:

1) $НОД(a,n)=1$;

2) $a^t \equiv 1 \bmod n$ или $\exists k$, число, $0\le k<r$, что $a^{2^k t}\equiv -1 \bmod n$

не превышает $n/4$.

Теорема 2 Если тест Рабина-Миллера выдает ответ «n - составное число», n действительно является составным. Вероятность ответа «не удалось определить» для составного числа n не превосходит 1/4.

Замечание Если n – простое, то условия 1 и 2 теоремы 1 выполняются для всех a, $0\le a\le n-1$. Если же n – составное, то для случайно выбранного a из промежутка $0\le a\le n-1$ вероятность выполнения обоих условий теоремы 1 не превосходит 1/4.

Поэтому, если для k случайных значений a мы проверим выполнение условий теоремы и не обнаружим, что n – составное, то будем считать, что n – простое с вероятностью, не меньшей, чем $1-(1/4)^k$.

Таким образом, если мы 100 раз применим тест Рабина-Миллера к числу n и получим 100 вариантов ответа «не удалось определить», то можно с большой вероятностью утверждать, что число n – простое. Более точно, вероятность получения ста ответов «не удалось определить» для составного числа не превышает $(1/4)^{100}$, т.е. практически равна нулю. Тем не менее, этот тест не дает доказательства того, что число n - простое.

Можно предложить следующий вероятностный тест простоты:

– выбираем случайное число a, $1\le a\le n-1$, проверяем с помощью алгоритма Евклида выполнение условия $НОД(a,n)=1$; если оно не выполняется, то n – составное;

– если $НОД(a,n)\ne 1$, то находим разложение $n-1=2^r t$, определяем параметр $0\le k<r$ и вычисляем a^t для $k=0$;

– если $a^t \equiv \pm 1 \bmod n$, то ответ не известен, тест можно повторить еще раз;

– в противном случае вычисляем $a^{2t}, \ldots, a^{2^{k-1}t} \bmod n$ до тех пор, пока не получится ответ $a^{2^k t} \equiv -1 \bmod n$;

– если ни одно из чисел не равно -1, то n – составное; если мы получили в результат -1, то ответ не известен, тест можно повторить тест еще раз.

5) тест Соловея-Штрассена

Этот тест основан на квадратичных вычетах.

Теорема Пусть n – нечетное составное число. Тогда количество целых чисел a, $0 \le a \le n-1$, удовлетворяющих условиям:

а) $НОД(a,n) \ne 1$,

б) $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) (\bmod n)$

не превышает $n/2$.

Следствие Если n – простое, то условия 1 и 2 теоремы, очевидно, выполняются для всех a, $0 \le a \le n-1$. Если же n – составное, то для случайно выбранного a из промежутка $0 \le a \le n-1$ вероятность выполнения обоих условий теоремы не превосходит 1/2. Поэтому, если для k случайных значений a мы проверим выполнение условий теоремы и не обнаружим, что n – составное, то будем считать, что n – простое с вероятностью, не меньшей чем $1-(1/2)^k$.

Можно предложить следующий вероятностный тест простоты:

– выбираем случайное число a, $1 \le a \le n-1$ и проверяем с помощью алгоритма Евклида условие $НОД(a,n) \ne 1$; если оно не выполняется, то n – составное;

– проверяем выполнимость сравнения (б);

– если сравнение выполняется, то ответ не известен, можно повторить тест еще раз.

Числа, удовлетворяющие сравнению (**), называются ***эйлеровымы псевдопростыми по основанию a***. В данном случае для аналога чисел Кармайкла, которые были бы составными и эйлеровыми псевдопростыми для всех элементов a, здесь нет.

Данный результат был независимо получен Д. Лемером (1976 г.), Р. Соловеем и В. Штрассеном (1977 г.). Сложность данного теста, как и теста, основанного на малой теореме Ферма, оценивается величиной $O(\log^2 n)$.

ЗАДАЧИ ДЛЯ САМОСТОЯТЕЛЬНОГО РЕШЕНИЯ

Вариант 1

1 Вычислить значение функции Эйлера $\varphi(2205)$.

2 Используя каноническую форму числа, найти

НОД (25392; 18630; 19872).

3 Используя расширенный алгоритм Евклида, найти НОД(a; b) и записать в линейной форме, если $a = 9881$, $b = 10\,000$.

4 Найти наименьший положительный вычет 2 052 *mod* 18

5 Используя арифметику остатков, найти вычет

262310 561 *mod* 13.

6 Найти вычет 3^{153} *mod* 23, используя цепочку сложений и теорему Эйлера.

7 Найти последние две цифры числа 14^{62}.

8 Найти последние три цифры числа 941^{2883}.

9 Решить сравнение $9881x = 1(\text{mod } 10\,000)$ с помощью расширенного алгоритма Евклида.

10 Решить систему сравнений с помощью китайской теоремы об остатках:

$$\begin{cases} x \bmod 12 = 7, \\ x \bmod 13 = 5, \\ x \bmod 19 = 10, \\ x \bmod 7 = 4. \end{cases}$$

11 Найти все квадратичные вычеты по модулю 19.

12 Найти символ Якоби J(13 550; 59 427 837).

13 Проверить «простоту» числа $n = 4087$, используя вероятностные методы на основе малой теоремы Ферма и теоремы Рабина-Миллера, если случайно выбраны для проверки числа $a_1 = 365$, $a_2 = 12$.

Вариант 2

1 Вычислить значение функции Эйлера $\varphi(2625)$.

2 Используя каноническую форму числа, найти

НОД (22253; 17493; 15827).

3 Используя расширенный алгоритм Евклида, найти НОД(a; b) и записать в линейной форме, если $a = 9667$, $b = 10\,000$.

4 Найти наибольший неположительный вычет 1763 *mod* 18.

5 Используя арифметику остатков, найти вычет

404 077 777 (*mod* 13).

6 Найти вычет 5^{130} *mod* 23, используя цепочку сложений и теорему Эйлера.

7 Найти последние две цифры числа 15^{61}.

8 Найти последние три цифры числа 847^{2106}.

9 Решить сравнение $9667x = 1(\text{mod } 10\,000)$ с помощью расширенного ал-

горитма Евклида.

10 Решить систему сравнений с помощью китайской теоремы об остатках:

$$\begin{cases} x \bmod 25 = 7, \\ x \bmod 18 = 8, \\ x \bmod 11 = 6, \\ x \bmod 7 = 4. \end{cases}$$

11 Найти все квадратичные вычеты по модулю 31.

12 Найти символ Якоби $J(31\,699; 16\,321\,513)$.

13 Проверить «простоту» числа $n = 4331$, используя вероятностные методы на основе малой теоремы Ферма и теоремы Рабина-Миллера, если случайно выбраны для проверки числа $a_1 = 522$, $a_2 = 11$.

Вариант 3

1 Вычислить значение функции Эйлера $\varphi(5145)$.

2 Используя каноническую форму числа, найти

НОД (15884; 29716; 10944).

3 Используя расширенный алгоритм Евклида, найти НОД(a; b) и записать в линейной форме, если $a = 9753$, $b = 10\,000$.

4 Найти наибольший отрицательный вычет 2 052 *mod* 18.

5 Используя арифметику остатков, найти вычет

294906 391 *mod* 11.

6 Найти вычет 7^{151} *mod* 23, используя цепочку сложений и теорему Эйлера.

7 Найти последние две цифры числа 16^{60}.

8 Найти последние три цифры числа 753^{4485}.

9 Решить сравнение 9 753 x=1(mod 10 000) с помощью расширенного алгоритма Евклида.

10 Решить систему сравнений с помощью китайской теоремы об остатках:

$$\begin{cases} x \bmod 15 = 10, \\ x \bmod 22 = 20, \\ x \bmod 13 = 4, \\ x \bmod 7 = 3. \end{cases}$$

11 Найти все квадратичные вычеты по модулю 23.

12 Найти символ Якоби $J(30\,917; 32\,152\,967)$.

13 Проверить «простоту» числа $n = 5251$, используя вероятностные методы на основе малой теоремы Ферма и теоремы Рабина-Миллера, если случайно выбраны для проверки числа $a_1 = 355$, $a_2 = 10$.

Вариант 4

1 Вычислить значение функции Эйлера $\varphi(4725)$.

2 Используя каноническую форму числа, найти

НОД (10647; 12675; 2548).

3 Используя расширенный алгоритм Евклида, найти НОД(a; b) и записать в линейной форме, если a = 9737, b = 10 000.

4 Найти наименьший положительный вычет 2 052 *mod* 19

5 Используя арифметику остатков, найти вычет

380275 159 *mod* 13.

6 Найти вычет 3^{215} *mod* 31, используя цепочку сложений и теорему Эйлера.

7 Найти последние две цифры числа 18^{59}.

8 Найти последние три цифры числа 659^{4902}.

9 Решить сравнение 9 737x =1 (mod 10 000) с помощью расширенного алгоритма Евклида.

10 Решить систему сравнений с помощью китайской теоремы об остатках:

$$\begin{cases} x \bmod 33 = 17, \\ x \bmod 25 = 11, \\ x \bmod 13 = 7, \\ x \bmod 14 = 5 \end{cases}$$

11 Найти все квадратичные вычеты по модулю 37.

12 Найти символ Якоби J(37 543; 25 757 125).

13 Проверить «простоту» числа $n = 5041$, используя вероятностные методы на основе малой теоремы Ферма, теоремы Рабина-Миллера, если случайно выбраны для проверки числа a_1= 265, a_2=16.

Вариант 5

1 Вычислить значение функции Эйлера $\varphi(3675)$.

2 Используя каноническую форму числа, найти

НОД (11025; 35035; 25025).

3 Используя расширенный алгоритм Евклида, найти НОД(a; b) и записать в линейной форме, если a=8577, b= 10 000.

4 Найти наибольший неположительный вычет

3681 *mod* 19.

5 Используя арифметику остатков, найти вычет

251 127 409 *mod* 11.

6 Найти вычет 5^{207} *mod* 37, используя цепочку сложений и теорему Эйлера.

7 Найти последние две цифры числа 22^{58}

8 Найти последние три цифры числа 561^{5289}.

9 Решить сравнение 8 577 x = 1 mod 10 000 () с помощью расширен-

ного алгоритма Евклида.

10 Решить систему сравнений с помощью китайской теоремы об остатках:

$$\begin{cases} x \bmod 13 = 5, \\ x \bmod 23 = 5, \\ x \bmod 17 = 11, \\ x \bmod 19 = 7. \end{cases}$$

11 Найти все квадратичные вычеты по модулю 19.

12 Найти символ Якоби $J(13\,550; 59\,427\,837)$.

13 Проверить «простоту» числа $n = 4717$, используя вероятностные методы на основе малой теоремы Ферма и теоремы Рабина-Миллера, если случайно выбраны для проверки числа $a_1 = 266$, $a_2 = 13$.

Вариант 6

1 Вычислить значение функции Эйлера $\varphi(7875)$.

2 Используя каноническую форму числа, найти

НОД (15048; 12474; 11088).

3 Используя расширенный алгоритм Евклида, найти НОД(a; b) и записать линейной форме, если $a = 9337$, $b = 10\,000$.

4 Найти наибольший отрицательный вычет

5 *mod* 19.

6 Используя арифметику остатков, найти вычет

7 198 034 853 *mod* 13.

8 Найти вычет 7^{183} *mod* 31, используя цепочку сложений и теорему Эйлера.

7 Найти последние две цифры числа 28^{57}.

8 Найти последние три цифры числа 467^{5699}.

9 Решить сравнение 8 797 x = 1 (mod 10 000) с помощью расширенного алгоритма Евклида.

10 Решить систему сравнений с помощью китайской теоремы об остатках:

$$\begin{cases} x \bmod 23 = 3, \\ x \bmod 31 = 3, \\ x \bmod 3 = 2, \\ x \bmod 7 = 5. \end{cases}$$

11 Найти все квадратичные вычеты по модулю 31.

12 Найти символ Якоби $J(31\,699; 16\,321\,513)$.

13 Проверить «простоту» числа $n = 4453$, используя вероятностные методы на основе малой теоремы Ферма и теоремы Рабина-Миллера, если случайно выбраны для проверки числа $a_1 = 143$, $a_2 = 25$.

Вариант 7

1 Вычислить значение функции Эйлера $\varphi(113400)$.

2 Используя каноническую форму числа, найти:

НОД (5734; 812; 120).

3 Используя расширенный алгоритм Евклида, вычислить НОД(a; b) и записать в линейной форме, если a = 24648, b= 2720.

4 Найти наименьший положительный вычет

$$2\ 720\ mod\ 17$$

5 Используя арифметику остатков, найти вычет

192 081 487 *mod* 11б

6 Найти вычет 3^{178} *mod* 37, используя цепочку сложений и теорему Эйлера.

7 Найти последние две цифры числа 32^{56}.

8 Найти последние три цифры числа 371^{6092}.

9 Решить сравнение 9 337 x = 1(mod 10 000) с помощью расширенного алгоритма Евклида;

10 Решить систему сравнений с помощью китайской теоремы об остатках:

$$\begin{cases} x \bmod 17 = 7, \\ x \bmod 23 = 7, \\ x \bmod 31 = 2, \\ x \bmod 5 = 3. \end{cases}$$

11 Найти все квадратичные вычеты по модулю 23.

12 Найти символ Якоби J(30 917; 32 152 967).

13 Проверить «простоту» числа $n = 4457$, используя вероятностные методы на основе малой теоремы Ферма и теоремы Рабина-Миллера, если случайно выбраны для проверки числа a_1= 369, a_2= 14.

Вариант 8

1 Вычислить значение функции Эйлера $\varphi(529200)$.

2 Используя каноническую форму числа, найти

НОД (15110; 2140; 106).

3 Используя расширенный алгоритм Евклида, найти НОД(a; b) и записать в линейной форме, если a = 8688, b = 1074.

4 Найти наибольший неположительный вычет

$$2\ 720\ mod\ 13.$$

5 Используя арифметику остатков, найти вычет

281 791 147 *mod* 17.

6 Найти вычет 7^{176} *mod* 37, используя цепочку сложений и теорему Эйлера.

7 Найти последние две цифры числа 26^{55}.

8 Найти последние три цифры числа 273^{7277}.

9 Решить сравнение 6 677x = 1(mod 10 000) с помощью расширенного алгоритма Евклида;

10 Решить систему сравнений с помощью китайской теоремы об остатках:

$$\begin{cases} x \bmod 11 = 7, \\ x \bmod 17 = 11, \\ x \bmod 7 = 5, \\ x \bmod 29 = 3. \end{cases}$$

11 Найти все квадратичные вычеты по модулю 37.

12 Найти символ Якоби J(37 543; 25 757 125).

13 Проверить «простоту» числа $n = 5043$, используя вероятностные методы на основе малой теоремы Ферма и теоремы Рабина-Миллера, если случайно выбраны для проверки числа a_1=135, a_2= 15.

Список литературы

1 Гашков, С. Б. Криптографические методы защиты информации: учебное пособие для студентов вузов, обучающихся по направлению «Прикладная математика и информатика» и «Информационные технологии» [Текст] / С. Б. Гашков, Э. А. Применко, М. А. Черепнев. – М. : Академия, 2010. – 298 с.

2 Расторгуев, С. П. Основы информационной безопасности [Текст]: учебное пособие для студентов вузов, обучающихся по специальностям «Комплексное обеспечение информационной безопасности автоматизированных систем» и «Информационная безопасность телекоммуникационных систем» / С. П. Расторгуев. – 2-е изд., стер. – М. : Академия, 2009. – 187 с.

3 Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей» [Текст] : учеб. пособие / В. Ф. Шаньгин. – М. : ИД «ФОРУМ»; ИНФРА-М, 2008. – 593 с.

4 Вейль, А. Основы теории чисел» [Текст] / А. Вейль; пер. с англ. Л. Н. Вассерштейн, А. Н. Паршин; ред. И. И. Пятецкий-Шапиро. – 2-е изд., стереотип. – М : УРСС, 2004. – 408 с.

5 Черемушкин, А. В. Вычисления в алгебре и теории чисел: курс лекций [Текст] : учебное пособие для студентов, обучающихся по специальности «Компьютерная безопасность» / А. В. Черемушкин. – М., 2002. – 123 с.

6 Зубов, А. Ю. Совершенные шифры: дополнительные главы курса криптографии [Текст] / А. Ю. Зубов. – М. : Гелиос АРВ, 2003. – 160 с.

7 Фомичев, В. М. Дискретная математика и криптология [Текст] : Курс лекций / В. М. Фомичев ; общ. ред. Н. Д. Подуфалова. – М. : ДИАЛОГ – МИФИ, 2003. – 400 с.

8 Лапонина, О. Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия: курс лекций [Текст]: учебное пособие для студентов вузов, обучающихся по специальности 510200 «Прикладная математика и информатика» / О. Р. Лапонина. – М. : Интернет университет информационных технологий, 2005 . – 605 с.

9 Столлингс, В. Криптография и защита сетей: принципы и практика [Текст] / В. Столлингс ; пер. с англ. – 2-е изд. – М. : Издательский дом «Вильямс», 2001. - 672 с.

10 Анин, Б. Ю. Защита компьютерной информации [Текст] / Б. Ю. Анин. – СПб. : БХВ – Санкт-Петербург, 2000. – 384 с.

11 Введение в криптографию / под общей ред. В. В. Ященко. – СПб. : Питер, 2001. – 288 с.

Змызгова Татьяна Рудольфовна

МАТЕМАТИЧЕСКИЕ ОСНОВЫ КРИПТОГРАФИИ. ТЕОРИЯ СРАВНЕНИЙ И ЕЕ ПРИЛОЖЕНИЯ

Методические указания и контрольные задания
по дисциплине «Криптографические методы защиты информации»
для студентов специальностей 090303.65, 231000.62

Редактор Е.А. Могутова

Подписано в печать | Формат 60x84 1/16 | Бумага тип. 65 гр.м^2
Печать цифровая | Усл. печ.л. 2,0 | Уч.-изд. л. 2,0
Заказ | Тираж э/в | Не для продажи

РИЦ Курганского государственного университета.
640669, г. Курган, ул. Советская, 63/4
Курганский государственный университет.