МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ

Л. В. Кнауб, Е. А. Новиков, Ю. А. Шитов

ТЕОРЕТИКО-ЧИСЛЕННЫЕ МЕТОДЫ В КРИПТОГРАФИИ

Рекомендовано Сибирским региональным учебно-методическим центром высшего профессионального образования для межвузовского использования в качестве учебного пособия для студентов, обучающихся по специальности 090102 «Компьютерная безопасность» и направлениям подготовки 090900 «Информационная безопасность» и 010200 «Математика и компьютерные науки» от 5 июля 2010 г.

Красноярск
СФУ
2011

УДК 519.72(075)
ББК 32.811я73
К53

Рецензенты:

И. О. Богульский, ведущий научный сотрудник ИВМ СОРАН, д-р физ.-мат. наук, проф.;

Ю. В. Шорников, д-р техн. наук, проф. кафедры АСУ новосибирского государственного технического университета

Кнауб, Л. В.

К53 Теоретико-численные методы в криптографии : учеб. пособие / Л. В. Кнауб, Е. А. Новиков, Ю. А. Шитов. – Красноярск : Сибирский федеральный университет, 2011. – 160 с.

ISBN 978-5-7638-2113-7

Излагаются некоторые элементы теории чисел, отношения сравнимости, модулярная арифметика, степенные вычеты, первообразные корни, индексы, алгоритмы дискретного логарифмирования, китайская теорема об остатках, простые числа и проверка на простоту, разложение чисел на множители и арифметические операции над большими числами. В прил. 1 описаны основы теории групп, колец и полей, а в прил. 2 приведены реализации некоторых алгоритмов, даны тексты программ на языке Borland C++, снабженные подробными комментариями.

Для студентов, обучающихся по специальности 090102 «Компьютерная безопасность» и направлениям подготовки 090900 «Информационная безопасность» и 010200 «Математика и компьютерные науки».

УДК 519.72(075)
ББК 32.811я73

Учебное издание

Кнауб Людмила Владимировна, Новиков Евгений Александрович
Шитов Юрий Александрович

ТЕОРЕТИКО-ЧИСЛЕННЫЕ МЕТОДЫ В КРИПТОГРАФИИ

Редактор Т. М. Пыжик
Компьютерная вёрстка Д. Р. Мифтахутдинова

Подписано в печать 06.06.2011. Печать плоская. Формат 60×84/16
Бумага офсетная. Усл. печ. л. 9,3. Тираж 100 экз. Заказ № 2481

Редакционно-издательский отдел Библиотечно-издательского комплекса
Сибирского федерального университета. 660041, г. Красноярск, пр. Свободный, 79

Отпечатано полиграфическим центром Библиотечно-издательского комплекса
Сибирского федерального университета. 660041, г. Красноярск, пр. Свободный, 82а

ISBN 978-5-7638-2113-7

ВВЕДЕНИЕ

Основой данного пособия является курс лекций по теоретико-численным методам в криптографии (ТЧМК). Этот курс предназначен для студентов ИКИТ кафедры прикладной математики и компьютерной безопасности, которые специализируются по информационной безопасности. Лекции по данному предмету формировались с 1996 года. Надо сказать, что в то время литературы на русском языке по таким направлениям, как защита информации, криптографии и математическим методам в криптографии практически не было (в отличии от зарубежных изданий). Поэтому на первом этапе «скелет» курса формировался на элементах теории чисел, алгоритмах арифметических операций с длинными числами и криптографических алгоритмах с открытыми ключами (RSA, схема Диффи – Хеллмана, схема Эль-Гамаля, схема аутентификации Шнора). Постепенно в тексты лекций, начиная с 2000 года, включались численные алгоритмы для решения трудных задач теории чисел. Для этого использовались переводы из зарубежных изданий по соответствующей тематике. В 2003 году Ю. А. Шитов издал методические указания по изучению численных алгоритмов для некоторых задач из теории чисел, которые использовались в курсе лекций по ТЧМК [15].

С 2001 года по направлениям «Криптография и математические методы в криптографии» начинают появляться учебные пособия и монографии на русском языке. В библиографическом списке приведен, по мнению авторов, достаточно полный обзор существующей литературы по этому направлению. В список не включены те учебники, в которых содержатся главы и разделы по арифметическим алгоритмам в теории чисел, так как любое учебное пособие по классическим курсам представляет собой аранжировку давно сформулированных и доказанных результатов, поэтому мы широко используем материалы из учебников, перечисленных в библиографическом списке.

Данное пособие отличается порядком и простотой изложения. Немного больше, чем в других пособиях, уделяется внимание решениям сравнений. Кроме того, при изложении результатов исключаются из рассмотрения доказательства некоторых трудных теорем, поскольку при желании слушатели курса могут ознакомиться с доказательствами в перечисленных источниках. При выборе материала авторы исходили из минимальных требований к начальной подготовке слушателей данного курса. Авторы предлагаемого пособия делают упор на возможность практической реализации изложенных алгоритмов на компьютере. Для некоторых алгоритмов, сформулированных в пособии, в приложении даны тексты программ, реализованных на языке BORLAND C++. Программы реализовал и тестировал М. В. Рыбков – студент группы ВТ 05–04, ИКИТ, СФУ.

Нумерация определений, теорем и соотношений приведены в разделах пособия.

НЕКОТОРЫЕ ЭЛЕМЕНТЫ ТЕОРИИ ЧИСЕЛ

В пособии не излагается теория чисел, а дан минимальный инструментарий из этой теории, который в дальнейшем потребуется для изучения криптографических систем, используемых в задачах по защите информации. Более подробное изложение математической теории чисел можно найти, например, в [1–2]. В теории чисел (по крайней мере, в той части, которая используется в криптографии) рассматривают целые числа и арифметические операции над ними. Перейдем к описанию основных понятий и определений из теории чисел [3].

Определение. Множество N натуральных чисел определяется с использованием аксиом Пеано:

1. $1 \in N$ (единица – натуральное число).

2. Для любого $a \in N$ существует единственное последующее $a^+ \in N$.

3. Для любого $a \in N$ выполняется неравенство $a^+ \neq 1$ (единица – наименьшее натуральное число).

4. Если $a^+ = b^+$, то $a = b$ (каждое последующее число обладает единственным предыдущим).

5. Если некоторое подмножество $N \subseteq \mathrm{N}$ содержит единицу и для каждого натурального числа $a \in N$ выполняется $a^+ \in N$, то $N = N$ (принцип индукции).

Таким образом, $N = \{1, 2, 3, 4, ...\}$.

На основании этих аксиом строится арифметика натуральных чисел, в которую включены операции сложения и умножения. Каждой паре натуральных чисел a, b можно единственным образом сопоставить их сумму – натуральное число $a + b$ так, чтобы выполнялись условия для любых натуральных чисел a, b, c:

1) $a + 1 = a^+$;

2) ассоциативность сложения: $(a + b) + c = a + (b + c)$;

3) коммутативность сложения: $a + b = b + a$;

4) если $a + b = a + c$, то $b = c$.

Каждой паре натуральных чисел a, b можно единственным образом сопоставить их произведение – натуральное число $a \cdot b$ так, чтобы выполнялись условия для любых натуральных чисел a, b, c:

1) $a \cdot 1 = a$;

2) $a \cdot b^+ = a \cdot b + a$;

3) ассоциативность умножения: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$;

4) коммутативность умножения: $a \cdot b = b \cdot a$;

5) дистрибутивность умножения относительно сложения:
$a \cdot (b + c) = a \cdot b + a \cdot c$, $(a + b) \cdot c = a \cdot c + b \cdot c$;

6) если $a \cdot b = a \cdot c$, то $b = c$.

Заметим, что множество натуральных чисел линейно упорядочено, т. е. для любых $a, b \in N$ выполняется ровно одно из условий: $a > b$, $a < b$, $a = b$.

Отношение < и > транзитивно, т. е. из неравенств $a < b$ и $b < c$ следует, что $a < c$. Если для $a, b \in N$ выполняется одно из соотношений $a > b$ или $a = b$, то записывают $a \leq b$ или $b \geq a$.

Определение. Множество Z целых чисел определим как объединение множеств натуральных чисел, отрицательных натуральных чисел и нуля. Таким образом

$$Z = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}.$$

На множестве Z целых чисел операции сложения и умножения задаются теми же правилами, что и для натуральных чисел.

Определение. Говорят, что целое число a делится (нацело) на целое число $b > 0$ (или что целое число $b > 0$ делит целое число a), если существует такое целое число c, что $a = bc$. Число a называют кратным числа b, число b – делителем числа a, число c – частным от деления a на b.

Пример. $8 = 4 \cdot 2$ (8 делится на 4 или 4 делит 8).

Отношение делимости обладает следующими свойствами.

1. Нуль делится на любое целое число.

2. Если a_1 делится на b, a_2 делится на b, то $a_1 + a_2$ делится на b.

3. Если $a_1 \pm a_2$ делится на b и a_1 делится на b, то a_2 делится на b.

4. Если a делится на b и x – произвольное целое число, то xa делится на b.

5. Любое целое число делится на 1.

6. Если a делится на b и b делится на c, то a делится на c.

7. Если 1 делится на a, то $a = \pm 1$.

Теорема 1. Для любого целого a и целого $b > 0$ существуют, и притом единственные, целые q и r, такие, что $a = bq + r$, $0 \leq r < b$.

Число r называют остатком от деления a на b. Если $r = 0$, то число q называют полным частным, в противном случае ($r \neq 0$) число q называют неполным частным.

Доказательство. Возьмем числа $b \cdot 1$, $b \cdot 2$, …, … При $a \geq 0$ среди этих чисел рассмотрим множество M тех, которые больше, чем a. Согласно аксиом Пеано, множество M не пусто. Следовательно, в этом множестве существует некоторое наименьшее число $b \cdot k$. Тогда справедливо неравенство $b \cdot k \leq a < b \cdot (k + 1)$.

При $a < 0$, $-a > 0$ можно рассмотреть множество M чисел $b \cdot i$ ($i = 1, 2, \ldots$), для которых выполняется неравенство $b \cdot i \geq -a$ и, соответственно, найти такое наименьшее число $b \cdot t'$, что при $t = t' - 1$ будет справедливо

$$bt < -a \leq b(t + 1),$$

так что

$$b(-t-1) \le a < b(-t).$$

Итак, для a и b ($b > 0$) существует целое q, такое, что

$$bq \le a < b(q+1).$$

В этом случае, обозначив через r разность $a–bq$, получаем

$$r = a - bq < b(q+1) - bq = b,\ r \ge 0,$$

так что $a = bq + r$, $0 \le r < b$.

Определение. Целое число $d \neq 0$ называется общим делителем целых чисел $a_1, a_2,\ldots a_k$, если каждое из чисел $a_1, a_2,\ldots a_k$ делится на d.

Пример. Числа 2, 3, 6 являются общими делителями чисел 12, 18, 36, 72.

Определение. Общий делитель $d \neq 0$ чисел $a_1, a_2,\ldots a_k$ называется наибольшим общим делителем (НОД) этих чисел, если d делится на любой другой общий делитель этих чисел.

Наибольший общий делитель чисел $a_1, a_2,\ldots a_k$ обозначается так: d = НОД($a_1, a_2,\ldots a_k$) или просто $d = (a_1, a_2,\ldots a_k)$.

Пример. Число 6 является наибольшим делителями чисел 12, 18, 36, 72, т. е. 6 = НОД (12, 18, 36, 72) или 6 = (12, 18, 36, 72).

Теорема. Для любых целых чисел, из которых хотя бы одно отлично от нуля, существует единственный НОД (см., например, [3]).

Теорема 2. Для любых целых чисел $a_1, a_2, ..., a_k$ наибольший общий делитель d можно представить в виде линейной комбинации этих чисел, т. е.

$$d = c_1a_1 + c_2a_2 + ... + c_ka_k,$$

где c_i – целые числа.

Доказательство [3]. Пусть $A = \{c_1a_1 + c_2a_2 + ... + c_ka_k\}$ – множество всевозможных целочисленных линейных комбинаций чисел $a_1, a_2, ..., a_k$. Будем считать, что не все числа $a_1, a_2, ..., a_k$ нулевые, тогда в множестве A существует наименьший положительный элемент. Обозначим его через d. Покажем, что множество A совпадает с множеством всех целых чисел, кратных d. Поскольку число d может быть представлено в виде линейной комбинации чисел $a_1, a_2, ..., a_k$, то и любое число вида x_id, где x_i – целые числа, может быть представлено в виде линейной комбинации этих чисел.

Обратно, любая линейная комбинация чисел $a_1, a_2, ..., a_k$ делится на d. Действительно, применим к числу d и произвольному элементу $y \in A$ теорему о делении с остатком: существуют такие целые числа q и r, что $y = qd + r$, причем $0 < r < d$. Число $r = y – qd$ является элементом множества A,

поскольку $y \in A$ и $d \in A$. Но d – наименьший неотрицательный элемент множества A, значит, $r = 0$ и $y = qd$. Таким образом, $A = \{x_i d\}$.

Осталось доказать, что d = НОД(a_1, a_2,… a_k). Каждое из этих чисел имеет вид $x_i d$, (x_i – целое число), что следует из комбинации вида

$$0 \cdot a_1 + 0 \cdot a_2 + ... + 0 \cdot a_{i-1} + 1 \cdot a_i + 0 \cdot a_{i+1}, + ... + 0 \cdot a_k).$$

Таким образом, d – общий делитель чисел a_1, a_2, ..., a_k. Пусть c – любой другой делитель этих чисел. Тогда по свойству 2 делимости c делит каждую линейную комбинацию вида $c_1a_1 + c_2a_2 + ... + c_ka_k$, в том числе и ту, которая равна d.

Из доказанной теоремы следует, что для любых не равных одновременно 0 чисел a, b существует два числа c, d такие, что НОД(a, b) = $= a \cdot c + b \cdot d$.

Определение. Целое число n называют простым, если $|n| \neq 1$ и единственными делителями числа n являются числа 1, –1, n, $-n$.

Если натуральное число p не делится ни на одно простое число $d \leq \sqrt{p}$, то число p – простое.

Определение. Натуральное число $p > 1$ называется составным, если число p имеет, по крайней мере, один положительный делитель, отличный от 1 и p.

Если число p составное, то справедлива следующая теорема.

Теорема. Для любого составного числа наименьший, отличный от 1, положительный делитель является простым числом.

Определение. Целые числа a_1, a_2, ..., a_k называются взаимно простыми в совокупности, если НОД(a_1, a_2, ..., a_k) = 1. Целые числа a и b называются взаимно простыми, если НОД(a, b) = 1.

Определение. Целые числа a_1, a_2, ..., a_k называются попарно взаимно простыми, если НОД(a_1, a_j) = 1 для всех $1 \leq i \neq j \leq k$.

Пример. Числа 3, 15, 6, 4 взаимно просты в совокупности, так как НОД(3, 15, 6, 4) = 1. Числа 3, 8, 17, 25, 121 попарно взаимно просты.

Теорема. Для того чтобы целые числа были взаимно просты, необходимо и достаточно, чтобы существовали такие целые числа,что $a \cdot c + b \cdot d = 1$.

Теорема 3 (основная теорема арифметики [3]). Всякое целое число n ($n \neq -1, 0, 1$) можно представить в виде $n = \varepsilon\, p_1\, p_2 ... p_r$, где $\varepsilon = \pm 1$ и p_1 ,p_2 ,..., p_r – простые числа (не обязательно различные), $r \geq 1$. Это представление единственно с точностью до порядка сомножителей.

Доказательство [3]. Сначала докажем, что разложение существует. Пусть n – целое число ($n \neq -1, 0, 1$). Доказывать будем индукцией по $|n|$. Если $|n| = 2$, то $n = \varepsilon \cdot 2$, $\varepsilon = \pm 1$. Пусть для всех целых чисел a ($a \neq -1, 0,1$), $|a| < |n|$, доказано существование нужного представления. Покажем, что для n такое представление тоже возможно. Если $|n|$ – простое число, то, обозначив его $|n| = p_1$, получим $n = \pm|n| = \pm \varepsilon p_1$, где $\varepsilon = \pm 1$.

Пусть теперь число n составное, $|n| > 1$, т. е. существует нетривиальный делитель a ($a \neq \pm 1$, $a \neq \pm n$) числа n. Тогда существует такое целое число b, что $n = ab$, где $b \neq \pm 1$, $b \neq \pm n$. Поскольку $|n| > 1$, справедливо равенство для абсолютных величин: $|n| = |ab| = |a| \cdot |b| > |a|$.

Аналогично $|n| > |b|$, поэтому к числам a и b применимо предположение индукции: $a = \varepsilon_1 p_1 p_2 \ldots p_k$, $b = \varepsilon_2 q_1 q_2 \ldots q_l$, где числа p_i , q_j простые, ε_1, $\varepsilon_2 = \pm 1$. Произведение $a \cdot b$ дает требуемое представление. Существование представления доказано.

Теперь покажем единственность. Пусть $n = \varepsilon_1 p_1 p_2 \ldots p_k = \varepsilon_2 q_1 q_2 \ldots q_l$, где числа p_i, q_j простые, $\varepsilon_1 = \pm 1$, $\varepsilon_2 = \pm 1$. Тогда $\varepsilon_1 = \varepsilon_2 = -1$ при $n < 0$. Далее, $p_1 p_2 \ldots p_k = q_1 q_2 \ldots q_l$, тогда по свойству 5 простых чисел $k = l$ и числа $q_1 q_2 \ldots q_l$ можно перенумеровать так, что $p_1 = q_1$, $p_2 = q_2, \ldots, p_k = q_l$.

Представление числа n в виде

$$n = p_1^{\alpha 1} p_2^{\alpha 2} \ldots p_s^{\alpha s},$$

где $\varepsilon = \pm 1$, $p_1, p_2, \ldots, p_s$ – различные простые числа, $\alpha_i \geq 1$ для $i = 1, 2, \ldots, s$, $s \geq 1$, называется каноническим разложением числа n.

ВЫЧИСЛЕНИЕ НАИБОЛЬШЕГО ОБЩЕГО ДЕЛИТЕЛЯ

Алгоритм Евклида

При работе с большими составными числами их разложение на простые множители, как правило, неизвестно. Но для многих прикладных задач теории чисел поиск разложения числа на множители является важной, часто встречающейся практической задачей. В теории чисел существует сравнительно быстрый способ вычисления НОД двух чисел, который называется алгоритмом Евклида.

Алгоритм 1. Алгоритм Евклида [3].

Вход. Целые числа a, b; $0 < b < a$.

Выход. d = НОД (a,b).

1. Положить $r_0 \leftarrow a$, $r_1 \leftarrow b$, $i \leftarrow 1$.
2. Найти остаток r_{i+1} от деления r_{i-1} на r_i.
3. Если $r_{i+1} = 0$, то положить $d \leftarrow r_i$. В противном случае положить $i \leftarrow i + 1$ и вернуться на шаг 2.
4. Результат: d.

Теорема. Для любых a, $b > 0$ алгоритм Евклида останавливается и выдаваемое им число d является наибольшим общим делителем чисел a и b.

Доказательство [3]. По теореме о делении с остатком для любого $i \geq 1$ имеем $r_{i-1} = q_i r_i + r_{i+1}$, где $0 \leq r_{i+1} < r_i$. Получаем монотонно убывающую последовательность неотрицательных целых чисел $r_1 > r_2 > r_3 > ... \geq 0$, ограниченную снизу. Такая последовательность не может быть бесконечной, значит, алгоритм Евклида останавливается.

Бинарный алгоритм Евклида

Бинарный алгоритм Евклида вычисления НОД оказывается более быстрым [3] при реализации этого алгоритма на компьютере, поскольку использует двоичное представление чисел a и b. Бинарный алгоритм Евклида основан на следующих свойствах наибольшего общего делителя (считаем, что $0 < b \leq a$):

1) если оба числа a и b четные, то НОД(a,b) = 2 · НОД(a/2 , b/2)
2) если число a нечетное, число b четное, то НОД(a, b) = НОД(a, b/2);
3) если оба числа a и b нечетные, $a > b$, то НОД(a, b) = НОД($a – b$, b);
4) если $a = b$, то НОД(a, b) = a.

Алгоритм 2. Бинарный алгоритм Евклида [3].

Вход. Целые числа a, b; $0 < b \leq a$.

Выход. d = НОД(a,b).

1. Положить $g \leftarrow 1$.

2. Пока оба числа a и b четные, выполнять $a \leftarrow a/2$, $b \leftarrow b/2$, $g \leftarrow 2g$ до получения хотя бы одного нечетного значения a или b.

3. Положить $u \leftarrow a$, $v \leftarrow b$.

4. Пока $u \neq 0$, выполнять следующие действия.

4.1. Пока u четное, полагать $u \leftarrow u/2$.

4.2. Пока v четное, полагать $v \leftarrow v/2$.

4.3. При $u \geq v$ положить $u \leftarrow u - v$.

В противном случае положить $v \leftarrow v - u$.

5. Положить $d \leftarrow gv$.

6. Результат: d.

Расширенный алгоритм Евклида

Расширенный алгоритм Евклида [3] находит наибольший общий делитель d чисел a и b и его линейное представление, т. е. целые числа x и y, для которых $ax + by = d$, и не требует «возврата», как в рассмотренном примере.

Пусть d – НОД для a и b, т. е. $d = (a, b)$, где $a > b$. Тогда существуют такие целые числа x и y, что $d = ax + by$. Иными словам, НОД двух чисел можно представить в виде линейной комбинации этих чисел с целыми коэффициентами.

Алгоритм 3. Схема расширенного алгоритма Евклида.

1. Определить $a_0 = 1$, $a_1 = 0$, $b_0 = 0$, $b_1 = 1$, $\alpha = a$, $\beta = b$.

2. Пусть число q – частное от деления числа a на число b, a число r – остаток от деления этих чисел (т. е. $a = qb + r$).

3. Если остаток от деления r равен нулю, то выполняем шаг 6.

4. Определяем:

$a = b$;
$b = r$;
$t = a_0$; // $t = x_{i-1}$
$a_0 = a_1$;
$a_1 = t - a_1 q$; // $a_1 = x_i$ – для правой части = x_{i+1} для правой
$t = b_0$; // $t = y_{i-1}$
$b_0 = b_1$;
$b_1 = t - b_1 q$;

5. Возвращаемся на шаг 2.

6. Определяем $x = x_0$, $y = y_0$, $d = \alpha x + \beta y$.

Вариант расширенного алгоритма Евклида

Вход. Целые числа a, b; $0 < b \leq a$.

Выход: d = НОД(a, b); такие целые числа x, y, что $ax + by = d$.

1. Положить $r_0 \leftarrow a$, $r_1 \leftarrow b$, $x_0 \leftarrow 1$, $x_1 \leftarrow 0$, $y_0 \leftarrow 0$, $y_1 \leftarrow 1$, $i \leftarrow 1$

2. Разделить с остатком r_{i-1} на r_i,: $r_{i-1} = q_i\, r_i + r_i + 1$

3. Если $r_{i+1} = 0$, то положить $d \leftarrow r_i$, $x \leftarrow x_i$ $y \leftarrow y_i$. В противном случае положить $x_{i+1} \leftarrow x_{i-1} - q_i x_i$, $y_{i+1} \leftarrow y_{i-1} - q_i y_i$, $i \leftarrow i + 1$ и вернуться на шаг 2.

4. Результат: d, x, y.

Корректность определения чисел x и y, вычисляемых алгоритмом, показывает следующая теорема.

Теорема 4. На каждой итерации алгоритма 3 выполняется равенство $ax_i + by_i = r_i$, при $i \geq 0$.

Доказательство [3]. Воспользуемся методом математической индукции. Для $i = 0$ и $i = 1$ требуемое равенство имеет место в силу шага 1 алгоритма 3. Допустим, что оно справедливо для $i - 1$ и для i. Тогда на шаге 3 получаем

$$x_{i+1} = x_{i-1} - q_i x_i \text{ и } y_{i+1} = y_{i-1} - q_i y_i.$$

Следовательно,

$$ax_{i+1} + by_{i+1} = a(x_{i-1} - q_i x_i) + b(y_{i-1} - q_i y_i,) =$$

$$= ax_{i-1} + by_{i-1} - q_i(ax_i + by_i) = r_{i-1} - q_i r_i = r_{i+1}.$$

Пример. Дано $a = 1769$, $b = 551$. Используя расширенный алгоритм Эвклида, найти целые числа x и y такие, что $d = ax + by$, где d – НОД чисел a и b.

I этап последовательности вычислений

1. Определить $a_0 = 1$, $a_1 = 0$, $b_0 = 0$, $b_1 = 1$, $\alpha = 1769$, $\beta = 551$.
2. Частное от деления $q = a/b = 1769/551 = 3$, а остаток от деления $r = 116$.
3. Если остаток от деления r равен нулю, то выполняем шаг 6.
4. Определяем:
   $a = 551$;
   $b = 116$;
   $t = a_0 = 1$;
   $a_0 = a_1 = 0$:
   $a_1 = t - a_1 q = 1 - 0 = 1$
   $t = b_0 = 0$;
   $b_0 = b_1 = 1$;
   $b_1 = t - b_1 q = -3$;

В результате текущего шага получили следующие промежуточные значения параметров:

$a = 551$, $b = 116$, $a_0 = 0$, $a_1 = 1$, $b_0 = 1$, $b_1 = -3$.

5. Так как остаток от деления $r \neq 0$, то возвращаемся на шаг 2.

II этап последовательности вычислений

1. Значение параметров:
   $a = 551$, $b = 116$, $a_0 = 0$, $a_1 = 1$, $b_0 = 1$, $b_1 = -3$.
2. Частное от деления $q = a/b = 551/116 = 4$, а остаток от деления $r = 87$.
3. Если остаток от деления r равен нулю, то выполняем шаг 6.
4. Определяем:
   $a = 116$;
   $b = 87$;
   $t = a_0 = 0$;
   $a_0 = a_1 = 1$:
   $a_1 = t - a_1 q = 0 - 1 \cdot 4 = -4$;
   $t = b_0 = 1$;
   $b_0 = b_1 = -3$;
   $b_1 = t - b_1 q = 1 - (-3) \cdot 4 = 13$;

В результате текущего шага получили следующие промежуточные значения параметров:

$a = 116$, $b = 87$, $a_0 = 1$, $a_1 = -4$, $b_0 = -3$, $b_1 = 13$.

5. Так как остаток от деления $r \neq 0$, то возвращаемся на шаг 2.

III этап последовательности вычислений

1. Значение параметров:
   $a = 116$, $b = 87$, $a_0 = 1$, $a_1 = -4$, $b_0 = -3$, $b_1 = 13$.
2. Частное от деления $q = a/b = 116/87 = 1$, а остаток от деления $r = 29$.
3. Если остаток от деления r равен нулю, то выполняем шаг 6.
4. Определяем:
   $a = 87$;
   $b = 29$;
   $t = a_0 = 1$;
   $a_0 = a_1 = -4$:
   $a_1 = t - a_1 q = 1 - (-4) \cdot 1 = 5$;
   $t = b_0 = -3$;
   $b_0 = b_1 = 13$;
   $b_1 = t - b_1 q = -3 - (13) \cdot 1 = -16$;

В результате текущего шага получили следующие промежуточные значения параметров:

$a = 87$, $b = 29$, $a_0 = -4$, $a_1 = 5$, $b_0 = 13$, $b_1 = -16$.

5. Так как остаток от деления $r \neq 0$, то возвращаемся на шаг 2.

IV этап последовательности вычислений.

1. Значение параметров:
   $a = 87$, $b = 29$, $a_0 = -4$, $a_1 = 5$, $b_0 = 13$, $b_1 = -16$.

2. Частное от деления $q = a/b = 87/29 = 3$, а остаток от деления $r = 0$.

3. Если остаток от деления r равен нулю, то выполняем шаг 6.

4. Определяем:

$a = 87$;

$b = 29$;

$t = a_0 = -4$;

$a_0 = a_1 = 5$; $-4 - 5 \cdot 3 = -19$;

$t = b_0 = 13$;

$b_0 = b_1 = -16$;

$b_1 = t - b_1 q = 13 - (-16) \cdot 3 = 61$;

В результате текущего шага получили следующие промежуточные значения параметров:

$a = 87$, $b = 29$, $a_0 = 5$, $a_1 = -19$, $b_0 = -16$, $b_1 = 61$.

5. Так как остаток от деления $r = 0$, то выполняем шаг 6.

6. Вычисляем НОД по формуле $d = \alpha x + \beta y$, где

$x = x_0 = 5$, $y = y_0 = -16$, $\alpha = 1769$, $\beta = 551$.

Подставляя значение параметров, получаем

$d = \alpha x + \beta y = 1769 \cdot 5 - 551 \cdot 16 = 8845 - 8816 = 29$.

Расширенный алгоритм Евклида можно реализовать и в двоичном виде.

Алгоритм 4. Расширенный бинарный алгоритм Евклида [3].

Вход. Целые числа a, b; $0 < b \le a$.

Выход. $d = $ НОД(a, b); такие целые числа x, y, что $ax + by = d$.

1. Положить $g \leftarrow 1$.

2. Пока оба числа a и b четные, выполнять $a \leftarrow a/2$, $b \leftarrow b/2$, $g \leftarrow 2g$ до получения хотя бы одного нечетного значения a или b.

3. Положить $u \leftarrow a$, $v \leftarrow b$, $A \leftarrow 1$, $B \leftarrow 0$, $C \leftarrow 0$, $D \leftarrow 1$.

4. Пока $u \neq 0$, выполнять следующие действия:

4.1. Пока u четное, положить $u \leftarrow u/2$.

4.1.2. Если оба числа A и B четные, то положить $A \leftarrow A/2$, $B \leftarrow B/2$.
В противном случае положить $A \leftarrow (A+b)/2$, $B \leftarrow (B-a)/2$

4.2. Пока v четное:

4.2.1. Положить $v \leftarrow v/2$.

4.2.2. Если оба числа C и D четные, то положить $C \leftarrow C/2$, $D \leftarrow D/2$.
В противном случае положить $C \leftarrow (C + b)/2$, $D \leftarrow (D - a)/2$

4.3. При $u \ge v$ положить $u \leftarrow u - v$, $A \leftarrow A - C$, $B \leftarrow B - D$.
В противном случае положить $v \leftarrow v - u$, $C \leftarrow C - A$, $D \leftarrow D - B$.

5. Положить $d \leftarrow gv$, $x \leftarrow C$, $y \leftarrow D$.

6. Результат: d, x, y.

ОТНОШЕНИЕ СРАВНИМОСТИ

Возьмем натуральное целое число m, которое будем называть модулем.

Определение. Целые числа a и b называются сравнимыми по модулю m, если разность $(a - b)$ делится на m ($m \mid a - b$).

Это соотношение между a, b и m для краткости записывается как $a \equiv b \bmod m$, где a и b будем называть соответственно левой и правой частями сравнения. Из определения 1 следует, что если a делится на m, то $a \equiv 0 \bmod m$.

Теорема 5. Число a сравнимо с b тогда и только тогда, когда a и b имеют одинаковые остатки при делении на модуль m.

Доказательство. Пусть $a \equiv b \ mod \ m$. Представим a и b в виде

$$a = mq^1 + r^1,\ b = mq^2 + r^2,$$

где $0 \le r^1 < m$, $0 \le r^2 < m$. Из этих представлений получаем

$$a - b = m(q^1 - q^2) + r^1 - r^2.$$

Так как $(m \mid a - b)$, то m должно делить $(r^1 - r^2)$. Однако имеет место – $m < r^1 - r^2 < m$. Отсюда следует, что $r^1 - r^2 = 0$, т. е. $r^1 = r^2$.

Обратно. Пусть остатки от деления a и b на m равны, т. е. имеет место $a = mq^1 + r$, $b = mq^2 + r$. Тогда $a - b = m(q^1 - q^2)$, т. е. $m \mid a - b$.

На основании теоремы можно дать следующее определение сравнимости чисел a и b.

Определение. Целые числа a и b называются сравнимыми по модулю m, если остатки от деления этих чисел на m равны.

Свойства сравнений

Теорема. Отношения сравнимости рефлексивно, т. е. $a \equiv a \bmod m$.

Доказательство следует из того, что левая и правая части сравнения имеют равные остатки.

Теорема 6. Отношения сравнимости симметрично, т. е. если $a \equiv b \bmod m$, то $b \equiv a \bmod m$.

Доказательство. Если a и b имеют одинаковые остатки при делении на m, то остатки от деления b и a на m также равны.

Теорема 7. Отношения сравнимости транзитивно, т. е. если $a \equiv b \bmod m$, $b \equiv c \bmod m$, то $a \equiv c \bmod m$.

Доказательство. Если у чисел a и b, а также у чисел b и c остатки от деления на m равны, то a и c имеют одинаковые остатки при делении на m.

Теорема 8. Если $a \equiv b \bmod m$ и k произвольное целое число, то $ka \equiv kb \bmod m$.

Доказательство. Если $a \equiv b \bmod m$, то $m|a - b$. Тогда $m|k(a - b)$ или $m|ka - kb$. Следовательно, $ka \equiv kb \bmod m$.

Определение. Пусть a и b целые числа, причем $b \neq 0$. Число b называется делителем a, если существует целое число k такое, что $a = kb$.

Определение. Общим делителем двух чисел a и b называется любое целое k, такое, что $k|a$ и $k|b$.

Определение. Наибольшим общим делителем (НОД) двух чисел a и b называется такой положительный общий делитель k, который делится на любой другой общий делитель этих чисел. Наибольший общий делитель чисел a и b обозначается следующим образом: $(a, b) = k$.

Определение. Числа a и b называются взаимно простыми, если наибольший общий делитель этих чисел равен 1, т. е. $(a,b) = 1$.

Теорема 9. Если $ka \equiv kb \bmod m$ и $(k,m) = 1$, то $a \equiv b \bmod m$.

Доказательство. Если $ka \equiv kb \bmod m$, то $m|ka - kb$, т. е. $m|k(a - b)$. Так как по условию вышеприведенных теорем наибольший общий делитель равен 1, то из условия $m|k(a - b)$ следует, что $m|a - b$.

Теорема. Если $a \equiv b \bmod m$ и k – произвольное целое натуральное число, то $ka \equiv kb \bmod km$.

Доказательство. Если $m|a - b$, то $km|ka - kb$. Отсюда следует, что $ka \equiv kb \bmod km$.

Теорема 10. Если $a \equiv b \bmod m$, $c \equiv d \bmod m$, то

$$a + c \equiv (b + d) \bmod m,\ a - c \equiv (b - d) \bmod m.$$

Доказательство. Если $m|a - b$ и $m|c - d$, то $m|(a - b) \pm (c - d)$. Отсюда получаем $m|(a \pm c) - (b \pm d)$.

Теорема. Если $a \equiv b \bmod m$, $c \equiv d \bmod m$, то $ac \equiv bd \bmod m$.

Доказательство. Если $a \equiv b \bmod m$ и $c \equiv d \bmod m$, то имеем

$$ac \equiv bc \bmod m \text{ и } cb \equiv db \bmod m.$$

Тогда из свойства транзитивности сравнений получим, что $ac \equiv bd \bmod m$.

Теорема 11. Если $a \equiv b \bmod m$, то при любом целом $n \geq 0$ имеет место $an \equiv bn \bmod m$.

Доказательство. Применяя n раз теорему 9 для сравнений $a \equiv b \bmod m$ и $a \equiv b \bmod m$, получим доказательство.

Пусть n – любое положительное целое число, $p(x)$ – многочлен степени n с целыми коэффициентами. Тогда из сформулированных выше теорем вытекает следующая теорема.

Теорема. Если $a \equiv b \bmod m$, то $p(a) \equiv p(b) \bmod m$.

МОДУЛЯРНАЯ АРИФМЕТИКА

Модулярная арифметика или арифметика остатков является основой современной криптографии. Эта арифметика заключается в том, что у любого выражения, в котором используются только целые числа, требуется вычислить не значение этого выражения, а остаток от деления этого значения на некоторое целое число n.

Арифметика остатков во многом совпадает с обычной арифметикой. Она коммутативна, ассоциативна и дистрибутивна. Кроме того, вычисление промежуточного результата по модулю n дает такой же результат, что и выполнение всего вычисления с последующим вычислением остатка, т. е. справедливы формулы

$$(a + b) \bmod n \equiv ((a \bmod n) + (b \bmod n)) \bmod n$$

$$(a - b) \bmod n \equiv ((a \bmod n) - (b \bmod n)) \bmod n$$

$$(a \cdot b) \bmod n \equiv ((a \bmod n) \cdot (b \bmod n)) \bmod n$$

$$(c(a + b)) \bmod n \equiv (((ca) \bmod n)+((cb) \bmod n)) \bmod n.$$

Пока при составлении арифметических выражений можно использовать только операции сложения, умножения и вычитания. В дальнейшем мы научимся вычислять обратный элемент, логарифм числа и квадратный корень по модулю n.

Вычисление $a^x \bmod n$

В случае, когда показатель степени x является степенью 2, для вычисления $a^x \bmod n$ можно использовать формулу, которая для $x = 16$ имеет следующий вид:

$$a^{16} \bmod n = (((a^2 \bmod n)^2 \bmod n)^2 \bmod n)^2 \bmod n.$$

Если показатель x не является степенью 2, то, записав этот показатель в двоичной системе счисления, можно представить x в виде суммы степеней 2, что позволяет значительно уменьшить число операций умножений.