Н. А. Молдовян

ТЕОРЕТИЧЕСКИЙ МИНИМУМ И АЛГОРИТМЫ ЦИФРОВОЙ ПОДПИСИ

- *Алгебраические структуры и вычислительные алгоритмы криптосистем с открытым ключом*
- *Синтез и анализ алгоритмов и протоколов электронной цифровой подписи (ЭЦП)*
- *Классические и новые схемы ЭЦП*
- *Стандарты ЭЦП, коллективная ЭЦП, слепая ЭЦП*
- *Открытое распределение ключей и коммутативное шифрование*
- *Патентование криптоалгоритмов*

УЧЕБНОЕ ПОСОБИЕ

Н. А. Молдовян

ТЕОРЕТИЧЕСКИЙ МИНИМУМ И АЛГОРИТМЫ ЦИФРОВОЙ ПОДПИСИ

Рекомендовано Учебно-методическим объединением высших учебных заведений Российской Федерации по образованию в области прикладных математики и физики в качестве учебного пособия для студентов, обучающихся по направлению "Прикладные математика и физика", а также смежным направлениям и специальностям в области математики и естественных наук и в области техники и технологии

Санкт-Петербург

«БХВ-Петербург»

2010

УДК 681.3.06(075.8)
ББК 32.973.26-018.2я73
М75

Молдовян Н. А.

М75 Теоретический минимум и алгоритмы цифровой подписи. — СПб.: БХВ-Петербург, 2010. — 304 с.: ил. — (Учебное пособие)

ISBN 978-5-9775-0585-7

Подробно рассмотрен минимальный математический аппарат, используемый при изучении криптосистем с открытым ключом, синтезе и анализе алгоритмов электронной цифровой подписи и коммутативного шифрования, протоколов открытого распределения ключей и открытого шифрования. Приводятся классические и новые криптосхемы с открытым ключом, их применение в информационных технологиях. Описываются стандарты ЭЦП, протоколы слепой и коллективной подписи. Рассмотрены различные способы задания конечных алгебраических структур, в том числе и некоммутативных, для синтеза алгоритмов ЭЦП и повышения их производительности. Отражены вопросы патентования криптоалгоритмов.

Для аспирантов, студентов и преподавателей высших учебных заведений

УДК 681.3.06(075.8)
ББК 32.973.26-018.2я73

Рецензент:
Р. М. Юсупов, член-корреспондент РАН, директор СПИИРАН

Группа подготовки издания:

Главный редактор	*Екатерина Кондукова*
Зам. главного редактора	*Евгений Рыбаков*
Зав. редакцией	*Григорий Добин*
Редактор	*Екатерина Капалыгина*
Компьютерная верстка	*Натальи Караваевой*
Корректор	*Виктория Пиотровская*
Дизайн серии	*Игоря Цырульникова*
Оформление обложки	*Елены Беляевой*
Зав. производством	*Николай Тверских*

Лицензия ИД № 02429 от 24.07.00. Подписано в печать 30.06.10.
Формат 70×100 1/16. Печать офсетная. Усл. печ. л. 24,51.
Тираж 1000 экз. Заказ №
"БХВ-Петербург", 190005, Санкт-Петербург, Измайловский пр., 29.

Санитарно-эпидемиологическое заключение
на продукцию № 77.99.60.953.Д.005770.05.09 от 26.05.2009 г. выдано Федеральной службой
по надзору в сфере защиты прав потребителей и благополучия человека.

Отпечатано с готовых диапозитивов
в ГУП "Типография "Наука"
199034, Санкт-Петербург, 9 линия, 12.

ISBN 978-5-9775-0585-7

Оглавление

Введение

Дисциплины, связанные с областью информационной безопасности, входят в программу подготовки специалистов широкого спектра различных направлений. Большое число вопросов обеспечения информационной безопасности и защиты информации связано с рассмотрением проблематики и методов криптографии. Изучение криптосистем с открытым ключом, к которым относятся алгоритмы и протоколы электронной цифровой подписи (ЭЦП), предполагает достаточно высокий уровень математической подготовки. Учитывая существенные различия в объеме преподаваемых математических дисциплин студентам различных направлений и специальностей, данное пособие написано таким образом, чтобы достаточно полно и глубоко ознакомить читателя с проблематикой современных схем ЭЦП при использовании минимального математического аппарата, главным образом результатов теории чисел. Такой подход был ранее испытан на примере книг "Введение в криптосистемы с открытым ключом" (БХВ-Петербург, 2005) и "Практикум по криптосистемам с открытым ключом" (БХВ-Петербург, 2007), которые стали достаточно известными в технических университетах России, используются в учебном процессе и получили признание в студенческой среде как учебные пособия, дружественно ориентированные на читателя без специальной математической подготовки.

Полученный опыт в значительной мере использован при написании данного учебного пособия, которое существенно расширяет изложение вопросов электронной цифровой подписи по сравнению с указанными ранее книгами. При этом рассматриваются не только алгоритмы и протоколы ЭЦП, ставшие уже классическими, а также и ряд новых вопросов, которые в настоящее время представлены только в специализированных научно-технических журналах. Целесообразность включения этого материала обосновывается тем, что он не сложен для понимания, имеет методическую ценность, предоставляет возможность формирования новых практических заданий при преподавании дисциплин, связанных с криптографией (криптографические методы защиты информации, теоретические основы криптографии, криптографические протоколы и др.) и способствует развитию исследовательских навыков и интереса к инновационной деятельности. Примером является *глава 7*, в ней рассматривается новая вычислительно трудная задача, которая формулируется над конечными некоммутативными группами, и способы построения групп такого типа. Данная задача связана с классической задачей дискретного логарифмирования (ЗДЛ), и ее можно охарактеризовать как ЗДЛ в скрытой циклической подгруппе конечной некоммутативной группы. Материал этой главы также не представляет трудности для понимания и расширяет представление о трудных задачах, используемых в синтезе криптосистем с открытым ключом.

Данная книга кратко излагает теоретико-числовые результаты *(глава 1)*, которые в дальнейшем активно востребованы при рассмотрении синтеза и анализа схем ЭЦП. Подробно изложены алгоритмы решения сложных задач, положенных в основу схем

ЭЦП и определяющих стойкость последних *(глава 2)*. Описывается ряд алгоритмов ЭЦП, ставших уже классическими *(глава 3)*. Детально раскрывается построение рандомизированных схем ЭЦП, основанных на сложности ЗДЛ *(глава 4)*, причем приводится большое число новых алгоритмов такого типа, которыми можно воспользоваться при выборе тем курсовых заданий. Представлены конечные мультипликативные группы с различным типом строения, задаваемые над конечными векторными пространствами, обсуждаются особенности их использования в синтезе алгоритмов ЭЦП и ЗДЛ в конечной группе с многомерным циклическим строением *(глава 5)*. Представлено применение схем ЭЦП для создания протоколов коллективной, композиционной и слепой коллективной подписи, включая их реализацию на основе двух вычислительно трудных задач, а также на основе официальных стандартов ЭЦП *(глава 6)*. Представлена в качестве криптографического примитива новая вычислительно трудная задача, в формулировке которой используется коммутативность операции возведения в степень и автоморфного отображения конечной некоммутативной группы, приведены криптосхемы на ее основе и рассмотрен вопрос задания конечных некоммутативных групп над конечными векторными пространствами *(глава 7)*. Полезным представляется также рассмотрение вопросов патентования криптографических алгоритмов и приводимые примеры формулы изобретения и описания изобретения *(глава 8)*. Описанная в общем виде картина процесса патентования и приводимый пример основных материалов патентной заявки на новый способ формирования и проверки ЭЦП дает понимание, как следует поступать при патентовании и других типов процедур обработки данных.

Книга ориентирована в первую очередь на студентов и преподавателей вузов, аспирантов и молодых специалистов, обучение, исследования и работа которых затрагивает вопросы информационной безопасности и электронного документооборота. Наличие в ней достаточного объема нового материала делает его интересным также и для специалистов из области криптографии.

Пособие может быть использовано в преподавании дисциплин "Криптографические методы защиты информации", "Теоретико-числовые методы в криптографии", "Теоретические основы компьютерной безопасности" и "Криптография" в рамках подготовки специалистов по следующим вузовским специальностям: "Компьютерная безопасность", "Организация и технология защиты информации", "Комплексное обеспечение информационной безопасности автоматизированных систем", "Многоканальные телекоммуникационные системы", "Защищенные системы связи", "Автоматизированные системы обработки информации и управления", "Прикладная математика" и др.

Автор выражает благодарность свои коллегам по исследованию новых криптографических примитивов, алгоритмов и протоколов Дерновой Е. С., Костиной А. А., Ананьеву М. Ю., Баженову А. А., Доронину С. Е., Галанову А. И., Гурьянову Д. Ю., Захарову Д. В., Куприянову И. А., Молдовяну Д. Н., Молдовяну П. А., Синеву В. Е., которые любезно предоставили материалы своих статей для использования в написанном учебном пособии. Данные материалы обладают нучно-технической новизной и являются одновременно прекрасным методическим материалом.

Глава 1

Элементы теории чисел

1.1. Некоторые определения и утверждения

Детальное рассмотрение приводимых в этой главе результатов теории чисел можно найти в работах [1—3].

Большую роль в теории чисел (и криптографии) играют простые числа. *Простым числом* называется число, которое делится без остатка только на единицу и само на себя. Иными словами, простым называется число $p \geq 3$, которое не делится без остатка ни на одно из следующих чисел 2, 3, …, $p - 1$. Число 2 также является простым.

Важным является также понятие взаимной простоты двух натуральных чисел. *Взаимно простыми* называются два целых положительных числа, наибольший общий делитель которых равен 1.

Сокращение в сравнениях множителей, являющихся взаимно простыми с модулем, основано на следующем утверждении.

Утверждение 1.1. Если НОД(a, n) = 1 и $(a \times b) \equiv (a \times c) \bmod n$, то $b \equiv c \bmod n$.

Доказательство. Из сравнения $(a \times b) \equiv (a \times c) \bmod n$ следует: $ab - ac \equiv 0 \bmod n \Rightarrow$ $\Rightarrow a(b - c) = Qn$, где Q — целое положительное число или 0. Если $Q = 0$, то утверждение выполняется. Если $Q \neq 0$, из равенства $a(b - c) = Qn$ следует, что в правой части содержится множитель n, который может содержаться только в значении $b - c$, поскольку a и n являются взаимно простыми числами, т. е. не содержат общих множителей, кроме 1. Таким образом, $b - c = qn$, где q — целое положительное число, т. е. $b \equiv c \bmod n$.

Пользуясь доказанным ранее утверждением, докажем следующее.

1.1.1. О существовании обратного элемента

Утверждение 1.2. Для любого целого числа $a > 0$ взаимно простого с модулем n существует обратное по mod n число, обозначаемое знаком a^{-1}, такое что $a \times a^{-1} \equiv 1 \bmod n$. Число a^{-1} называется мультипликативно обратным по модулю n.

Доказательство. Рассмотрим множество значений {1, 2, …, $n - 1$}. Умножая каждое из них на a по mod n, получаем множество {($a \bmod n$), ($2a \bmod n$), …,

$((n-1)\ a \bmod n)\}$, которое содержит по одному разу числа 1, 2, …, $n-1$, т. е. для некоторого значения i выполняется условие $ia \bmod n = 1$. Это вытекает из противоречия, возникающего при предположении о существовании двух одинаковых значений. Пусть, например, $ha \bmod n = ka \bmod n$. Тогда с учетом условия НОД$(a, n) = 1$ из последнего условия получаем $h \equiv k \bmod n \Rightarrow h = k$. Последнее противоречит тому, что мы умножали на a только различные числа. Указанное значение i и является мультипликативно обратным (к числу a) элементом по модулю n.

Следствие 1.1. Если модуль p является простым числом, то для любого числа $0 < a < p$ существует мультипликативно обратный элемент по модулю p.

Можно показать, что если НОД$(a, n) \neq 1$, то не существует числа b, такого что $ab \equiv 1 \bmod n$. Действительно, пусть НОД$(a, n) = d$, т. е. $a = dq$ и $n = dp$. Умножая на a по модулю n каждое число из множества значений $\{1, 2, \ldots, dp-1\}$, получим следующий ряд остатков $\{(a \bmod n),\ (2a \bmod n), \ldots, ((dp-1)\ a \bmod n)\}$. Покажем, что каждый из этих остатков делится без остатка на d, т. е. содержит множитель d. Возьмем любое число b, такое что $0 < b < dp$, и вычислим остаток от деления ab на n: $r = ab - Qn = dqb - Qdp = d(qb - Qp)$, где Q — некоторое натуральное число. Из равенства $r = d(qb - Qp)$ следует, что остаток r делится на d. (Одновременно мы доказали утверждение о делимости остатка, которое сформулировано далее.) Таким образом, в указанном ряде $n-1$ остатков содержатся только остатки, делящиеся нацело на d. Поскольку среди них нет 1, то это означает, что не существует числа b, при котором $ab \equiv 1 \bmod n$. Что мы и хотели показать.

1.1.2. О делимости остатка

Утверждение 1.3. Пусть для целых положительных чисел a и b имеем $a > b$ и НОД$(a, b) = d$, тогда для остатка r от деления a на b выполняется равенство НОД$(b, r) = d$.

Данное утверждение лежит в основе алгоритма Евклида, позволяющего быстро вычислять наибольший общий делитель двух целых положительных чисел.

1.1.3. Теорема Ферма

Теорема Ферма утверждает следующее: для любого простого числа p и любого положительного числа a, которое не делится на p, выполняется сравнение:

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

Доказательство. Рассмотрим множество чисел $\{1,2, \ldots, p-1\}$, которое обозначим как $\mathbb{Z}_p$. Если все элементы $\mathbb{Z}_p$ умножить на a по модулю p, то, используя утверждение 1, легко показать, что в результате получим некоторую перестановку элементов $\mathbb{Z}_p$. Иными словами, в наборе $\{a \bmod p, 2a \bmod p, \ldots, (p-1)a \bmod p\}$ содержится $(p-1)$ различных чисел, т. е. каждое из чисел 1, 2, ..., $p-1$ встречается ровно по одному разу. Перемножая числа a, $2a$, ..., $(p-1)a$, получаем:

$$a \times 2a \times \ldots \times (p-1)a = (p-1)!\ a^{p-1}.$$

Поделив на p левую и правую части последнего соотношения, получим:

$$[a \times 2a \times \ldots \times (p-1)a] \bmod p = (p-1)!\ a^{p-1} \bmod p;$$

$$(a \bmod p) \times (2a \bmod p) \times \ldots \times ((p-1)a \bmod p) \equiv (p-1)!\ a^{p-1} \bmod p.$$

Поскольку от перестановки мест сомножителей произведение не изменяется, то левую часть последнего сравнения можно представить в виде:

$$[(a \bmod p) \times (2a \bmod p) \times \ldots \times ((p-1)a \bmod p)] =$$

$$= 1 \times 2 \times \ldots \times (p-1) = (p-1)!$$

Из последних двух соотношений следует:

$$(p-1)! \equiv (p-1)!\ a^{p-1} \bmod p.$$

Числа $(p-1)!$ и p являются взаимно простыми, поэтому в последнем выражении на основании утверждения 1 можно левую и правую части сократить на $(p-1)!$, откуда вытекает сравнение:

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

Теперь не представляет труда вывести следующие формулы:

$$a^p \equiv a \bmod p$$

$$b \equiv c \bmod (p-1) \Rightarrow a^b \equiv a^c \bmod p.$$

1.2. Функция Эйлера

В обобщении теоремы Ферма используется понятие функции Эйлера, которая часто будет нам встречаться в дальнейшем. Функция Эйлера играет важную роль в теории чисел. Она обозначается символом $\varphi(n)$ и определяется как число положительных целых чисел, которые меньше n и являются взаимно простыми с n.

Очевидно, что для простого p имеем $\varphi(p) = p - 1$. Используя утверждение о мультипликативности функции Эйлера, для числа $n = pq$, являющегося произведением двух простых чисел p и q, можно легко получить:

$$\varphi(n) = \varphi(pq) = \varphi(p) \times \varphi(q) = (p-1) \times (q-1).$$

Эту частную формулу легко получить и без использования свойства мультипликативности функции Эйлера. Действительно, рассмотрим множество чисел $\{1, 2, \ldots, (pq-1)\}$. Нетрудно заметить, что все числа, которые не превышают значение pq и не являются взаимно простыми с $pq = n$, составляют следующие два множества $\{p, 2p, \ldots, (q-1)p\}$ и $\{q, 2q, \ldots, (p-1)q\}$. В первом содержится $q - 1$, а во втором $p - 1$ различных чисел. Вычитая из $n - 1$ значения $q - 1$ и $p - 1$, получим:

$$\varphi(n) = pq - 1 - (q-1) - (p-1) = pq - (p+q) + 1 = (p-1) \times (q-1).$$

Однако в общем случае, когда в каноническом разложении числа n содержится сравнительно большое число простых сомножителей и их степеней, при вычислении функции Эйлера используется то, что она является мультипликативной функцией, т. е. для двух взаимно простых чисел a и b выполняется соотношение $\varphi(ab) = \varphi(a) \times \varphi(b)$.

Поскольку в каноническом разложении произвольного числа n содержатся только взаимно простые сомножители вида p^s, где $s \geq 1$, то для вычисления функции Эйлера достаточно научиться вычислять функцию Эйлера от чисел вида p^s и уметь разлагать число n на простые множители.

Пусть дано число p^s. Рассмотрим множество чисел:

$$\{1, 2, \ldots, p, \ldots, 2p, \ldots, 3p, \ldots, p^{s-1}p\}.$$

Нетрудно заметить, что все числа, входящие в это множество и не являющиеся взаимно простыми с p^s, составляют подмножество $\{p, 2p, 3p, \ldots, p^{s-1}p\}$ из p^{s-1} чисел. Отсюда получаем:

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

Используя эту формулу и свойство мультипликативности, можно легко вычислить функцию Эйлера от произвольного заданного числа, если нам удастся разложить его на множители.

Теорема Эйлера. Теорема Эйлера, являющаяся обобщением теоремы Ферма, утверждает, что для любых взаимно простых чисел a и n выполняется сравнение:

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

Доказательство. Доказательство аналогично доказательству теоремы Ферма. Поскольку для простого n имеем $\varphi(n) = (n-1)$, то в этом случае сравнение $a^{\varphi(n)} \equiv 1 \bmod n$ непосредственно следует из теоремы Ферма (является просто другой формой записи последней). Доказательство для произвольного n опирается на определение функции Эйлера: $\varphi(n)$ равно числу положительных целых чисел, меньших n и взаимно простых с n. Множество таких целых чисел включает $\varphi(n)$ значений, которые можно пронумеровать следующим образом:

$$\Phi = \{x_1, x_2, \ldots, x_{\varphi(n)}\}.$$

Умножая каждый элемент этого множества на a по модулю n, получим множество:

$$\Phi' = \{(ax_1 \bmod n), (ax_2 \bmod n), \ldots, (ax_{\varphi(n)} \bmod n)\}.$$

Покажем, что последние два множества включают одни и те же элементы. Действительно, для всех значений $i = 1, 2, \ldots, \varphi(n)$ числа a и x_i являются взаимно простыми с n, поэтому число ax_i тоже является взаимно простым с n. Следовательно, все элементы Φ' являются целыми числами, меньшими n (умножение мы выполняли по модулю n) и взаимно простыми с n. В множестве Φ' нет повторений, так как если $(a \times b) \equiv (a \times c) \bmod n$, то $b \equiv c \bmod n$, поскольку по условию доказываемой теоремы a и n являются взаимно простыми числами. Действительно, из условия $ax_i \bmod n = ax_j \bmod n$ следует $x_i = x_j$, что противоречит тому, что в множестве Φ все числа различны. Таким образом, множества Φ и Φ' содержат одни и те же элементы. Перемножая все элементы множества Φ', а затем все элементы множества Φ, получаем равенство:

$$\prod_{i=1}^{\varphi(n)} (ax_i \bmod n) = \prod_{i=1}^{\varphi(n)} x_i,$$

из которого следуют сравнения:

$$\prod_{i=1}^{\varphi(n)} ax_i \equiv \prod_{i=1}^{\varphi(n)} x_i \pmod{n},$$

$$a^{\varphi(n)} \times \left[\prod_{i=1}^{\varphi(n)} x_i \right] \equiv \prod_{i=1}^{\varphi(n)} x_i \pmod{n},$$

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

Из последнего сравнения вытекают следующие соотношения:

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

$$b \equiv c \bmod \varphi(n) \Rightarrow a^b \equiv a^c \bmod n.$$

1.2.1. Обобщенная теорема Эйлера

Обобщенной функцией Эйлера называется функция $L(n)$, определенная для всех натуральных чисел следующим образом: $L(1) = 1$, а при $n > 1$

$$L(n) = \text{НОК}\left[p_1^{\alpha_1 - 1}(p_1 - 1); p_2^{\alpha_2 - 1}(p_2 - 1); \ldots; p_k^{\alpha_k - 1}(p_k - 1) \right],$$

где $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ и НОК — наименьшее общее кратное.

Обобщенная теорема Эйлера. Если НОД(a, n) = 1, то

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

Доказательство. Пусть $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ — каноническое разложение числа n. По теореме Эйлера $\forall\, i \in \{1, 2, \ldots, k\}$ имеем: $a^{p_i^{\alpha_i - 1}(p_i - 1)} \equiv 1 \bmod p_i^{\alpha_i}$. Возводя обе части последнего сравнения в целочисленную степень $\dfrac{L(n)}{p_i^{\alpha_i - 1}(p_i - 1)}$ (последнее число является целым, так как по определению $p_i^{\alpha_i - 1}(p_i - 1) \mid L(n)$), получаем: $\forall\, i \in \{1, 2, \ldots, k\}$ имеет место $a^{L(n)} \equiv 1 \bmod p_i^{\alpha_i}$. Так как $\forall\, i, j \in \{1, 2, \ldots, k\}$ $(i \neq j)$ числа $p_i^{\alpha_i}$ и $p_j^{\alpha_j}$ являются взаимно простыми, то по теореме 12 *(см. разд. 1.7)* имеем $a^{L(n)} \equiv 1 \bmod n$.

1.3. Алгоритм Евклида

Пусть **MOD**(a, b) есть операция взятия остатка от деления a на b, а **QUO**(a, b) есть частное от деления a на b. Алгоритм Евклида позволяет без разложения двух целых чисел на множители находить их наибольший общий делитель. В данном алгоритме используется следующее утверждение: если $a = bq + r$, где $b \neq 0$, и число d де-

лит a и b, то оно делит и r, т. е. имеем $d \mid (a - bq)$. Это утверждение верно для любого делителя, включая наибольший общий делитель d = НОД(a, b). Отсюда следует, что НОД(a,b) = НОД [b, **MOD** (a, b)].

Для всякого a имеем также НОД(a, 0) = $|a|$. Пусть задано целое число a и ненулевое целое число b. Алгоритм Евклида предполагает выполнение следующей последовательности делений, где принято обозначение $a_0 = a$ и $a_1 = b$:

$$\begin{aligned}
a_0 &= a_1 q_1 + a_2, && 0 < a_2 < |a_1|,\\
a_1 &= a_2 q_2 + a_3, && 0 < a_3 < a_2,\\
&\ldots\\
a_{k-2} &= a_{k-1} q_{k-1} + a_k, && 0 < a_k < a_{k-1},\\
a_{k-1} &= a_k q_k + 0.
\end{aligned}$$

Процесс деления имеет конечное число шагов, поскольку остатки убывают по абсолютной величине $|a_1| > a_2 > a_3 > \ldots > 0$ (значение a_1 может быть отрицательным, поэтому оно взято по абсолютной величине; остальные остатки положительны). Значение a_k является наибольшим общим делителем. С учетом указанного ранее утверждения имеем

$$\text{НОД}(a_0, a_1) = \text{НОД}(a_1, a_2) = \ldots = \text{НОД}(a_k, 0) = a_k,$$

т. е. на самом деле a_k является наибольшим общим делителем чисел a и b. Одновременно мы показали, что приведенный далее алгоритм работает правильно.

Обозначим операцию присвоения следующим образом: $x := y$ означает присвоение переменной x значения y, а $(x, y) := (x_1, y_1)$ означает выполнение операций $x := x_1$ и $y := y_1$.

Алгоритм Евклида (нахождение НОД(a, b)).

ВХОД: a и $b \neq 0$.

1. [Инициализация] $(a_0, a_1) := (a, b)$.

2. [Основной цикл] Пока $a_1 \neq 0$ выполнять

   $(a_0, a_1) := [a_1,$ **MOD** $(a_0, a_1)]$.

3. Вернуть $d := a_0$.

ВЫХОД: d = НОД(a, b).

1.4. Расширенный алгоритм Евклида

В любой строке описанного ранее алгоритма Евклида каждый остаток является линейным представлением делимого и делителя. Легко видеть, что, начиная с одного из ненулевых остатков (например, последнего, т. е. начиная с a_k) и выражая остатки, полученные на последующих шагах алгоритма Евклида, через остатки, полученные на предыдущих шагах, можно представить значение a_i (соответственно, a_k) в следующем виде $a_i = ax' + by'$ (соответственно, $a_k = ax + by$), где x и y —некоторые целочисленные коэффициенты. Расширенный алгоритм Евклида позволяет вычис-

лить значения коэффициентов x и y в указанном линейном представлении НОД(a, b), т. е. в выражении $a_k = ax + by$. Работа расширенного алгоритма Евклида организуется так, что значения x' и y' вычисляются в серии шагов, в каждом из которых мы выражаем a_i в виде указанного линейного представления.

Каждый остаток, вычисленный в процессе работы алгоритма Евклида, можно представить в виде $ax_i + by_i$. Рассмотрим следующую последовательность такого представления остатков:

$$\begin{aligned}
&a_0 = a, && a_0 = ax_0 + by_0,\\
&a_1 = b, && a_1 = ax_1 + by_1,\\
&a_2 = a_0 - a_1 q_1, && a_2 = ax_2 + by_2,\\
&\dots\\
&a_i = a_{i-2} - a_{i-1} q_{i-1}, && a_i = ax_i + by_i,\\
&\dots\\
&a_k = a_{k-2} - a_{k-1} q_{k-1}, && a_k = ax_k + by_k,\\
&0 = a_{k-1} - a_k q_k, && 0 = ax_{k+1} + by_{k+1}.
\end{aligned}$$

В левом столбце фактически приведена последовательность делений, полученная в алгоритме Евклида, но записанная в виде выражения для вычисления остатков. В правом столбце каждый остаток выражен в интересующем нас виде $ax_i + by_i$. Пока мы не знаем коэффициентов. Нашей целью является вычисление x_i и y_i для любого i, а следовательно, и для $i = k$. Очевидно, что $x_0 = 1$, $y_0 = 0$ и $x_1 = 0$, $y_1 = 1$. Сравнивая обе части на i-м шаге, получаем:

$$\begin{aligned}
a_i = ax_i + by_i = a_{i-2} - a_{i-1}q_{i-1} = (ax_{i-2} + by_{i-2}) - (ax_{i-1} + by_{i-1})q_{i-1} =\\
= a(x_{i-2} - x_{i-1}q_{i-1}) + b(y_{i-2} - y_{i-1}q_{i-1}),
\end{aligned}$$

откуда получается следующая индуктивная процедура вычисления x_i и y_i:

$$\begin{aligned}
q_{i-1} &= \mathbf{QUO}(a_{i-2}, a_{i-1}),\\
a_i &= a_{i-2} - a_{i-1}q_{i-1},\\
x_i &= x_{i-2} - x_{i-1}q_{i-1},\\
y_i &= y_{i-2} - y_{i-1}q_{i-1}.
\end{aligned}$$

Отметим, что значение a_i может быть вычислено как MOD(a_{i-2}, a_{i-1}), но достоинство приведенного ранее выражения заключается в том, что a_i вычисляется аналогично вычислению коэффициентов x_i и y_i. Этот факт используется в следующем алгоритме.

Расширенный алгоритм Евклида.

ВХОД: a и $b \neq 0$.

1. [Инициализация] $(a_0, a_1) := (a, b)$; $(x_0, x_1) := (1, 0)$; $(y_0, y_1) := (0, 1)$.

2. [Основной цикл] Пока $a_1 \neq 0$ выполнять:

   {$q := \mathbf{QUO}(a_0, a_1)$;

   $(a_0, a_1) := (a_1, a_0 - a_1 q)$;

$(x_0, x_1) := (x_1, x_0 - x_1 q)$;

$(y_0, y_1) := (y_1, y_0 - y_1 q)\}$.

3. Вернуть $(d, x, y) := (a_0, x_0, y_0)$.

ВЫХОД: d, x, y, такие что $d = \text{НОД}(a, b) = ax + by$.

1.5. Показатели и первообразные корни

Для взаимно простого с модулем n числа a, согласно теореме Эйлера, существует некоторое положительное $\gamma = \varphi(n)$, для которого выполняется условие $a^{\gamma} \equiv 1 \pmod{n}$. В случае простого модуля p имеем $\gamma = p - 1$. Представляет интерес найти наименьшее из чисел γ, для которых выполняется указанное условие.

Определение. Пусть $\text{НОД}(a, n) = 1$. Наименьшее из чисел γ, для которых выполняется сравнение $a^{\gamma} \equiv 1 \pmod{n}$, называется *показателем*, которому число a принадлежит по модулю n.

Утверждение 1.4. Если a по модулю n принадлежит показателю δ, то числа $a^0, a^1, \ldots, a^{\delta - 1}$ по модулю n несравнимы.

Доказательство. Пусть $a^h \equiv a^k \pmod{n}$, $0 \le k < h < \delta$. Тогда получим $a^{h-k} \equiv 1 \pmod{n}$, где $0 < h - k < \delta$. Но, по определению, δ есть наименьшее из чисел γ, для которых выполняется сравнение $a^{\gamma} \equiv 1 \pmod{n}$. Противоречие доказывает утверждение.

Утверждение 1.5.

а) Если a по модулю n принадлежит показателю δ, то $a^{\gamma} \equiv a^{\gamma'} \pmod{n}$ тогда и только тогда, когда $\gamma \equiv \gamma' \pmod{\delta}$.

б) Если $\gamma \ne 0$, то имеем сравнение $a^{\gamma} \equiv 1 \pmod{n}$, которое выполняется тогда и только тогда, когда γ делится на показатель δ.

Доказательство. Пусть r и r' есть наименьшие неотрицательные вычеты чисел γ и γ' по модулю δ. Тогда при некоторых q и q' имеем: $\gamma = \delta q + r$, $\gamma' = \delta q' + r'$. Поскольку $a^{\delta} \equiv 1 \pmod{n}$, то получаем $a^{\gamma} = (a^{\delta})^q a^r \equiv a^r \pmod{n}$ и $a^{\gamma'} = (a^{\delta})^{q'} a^{r'} \equiv a^{r'} \pmod{n}$.

Следовательно, $a^{\gamma} \equiv a^{\gamma'} \pmod{n}$ тогда и только тогда, когда $a^r \equiv a^{r'} \pmod{n}$, т. е. тогда и только тогда, когда $r = r'$. (Действительно, $r < \delta$ и $r' < \delta$ и из $a^r \equiv a^{r'} \pmod{n}$ следует $r = r'$. В противном случае имеем противоречие: $a^{|r - r'|} = 1 \pmod{n}$ при $0 < |r - r'| < \delta$.)

Следствие 1.2. Показатели, которым числа a принадлежат по модулю n, являются делителями $\varphi(n)$.

Действительно, пусть a по модулю n принадлежит показателю δ. Из $a^{\varphi(n)} \equiv 1 \pmod{n}$ следует, что $\varphi(n)$ делится на δ. Наибольший из этих делителей есть само $\varphi(n)$.

1.5.1. Первообразные корни

Интересен вопрос о существовании чисел, принадлежащих показателю $\varphi(n)$. Такие числа существуют и называются первообразными корнями по модулю n.

Утверждение 1.6. Если число a по модулю n принадлежит показателю $\varepsilon'\varepsilon$, то $a^{\varepsilon'}$ принадлежит показателю ε.

Доказательство. Действительно, пусть $a^{\varepsilon'}$ принадлежит показателю δ. Тогда $(a^{\varepsilon'})^{\delta} \equiv 1 \pmod{n}$, т. е. $a^{\varepsilon'\delta} \equiv 1 \pmod{n}$, из чего следует, что $\varepsilon'\delta$ делится на $\varepsilon'\varepsilon$, т. е. δ делится на ε. С другой стороны, $a^{\varepsilon'\varepsilon} \equiv 1 \pmod{n}$, откуда $(a^{\varepsilon'})^{\varepsilon} \equiv 1 \pmod{n}$), откуда, по утверждению 5, следует, что ε делится на δ. Таким образом, $\varepsilon \mid \delta$ и $\delta \mid \varepsilon$, поэтому $\delta = \varepsilon$.

Утверждение 1.7. Если a по модулю n принадлежит показателю u, а b — показателю v, причем НОД $(u, v) = 1$, то *ab принадлежит показателю uv*.

Доказательство. Действительно, пусть ab принадлежит показателю δ. Тогда $(ab)^{\delta} \equiv 1 \pmod{n} \Rightarrow (ab)^{v\delta} \equiv 1 \pmod{n} \Rightarrow a^{v\delta}b^{v\delta} \equiv 1 \pmod{n} \Rightarrow a^{v\delta} \equiv 1 \pmod{n}$, откуда следует, что $v\delta$ делится на u. Но поскольку НОД $(u, v) = 1$, то δ делится на u. Рассуждая аналогичным образом, получим, что δ делится на v. Ввиду того, что $u \mid \delta$, $v \mid \delta$ и НОД$(a, b) = 1$, то $(uv) \mid \delta$, т. е. δ делится и на uv. С другой стороны, из $a^u b^v \equiv (a^u)^v (b^v)^u \equiv (ab)^{uv} \equiv 1 \pmod{n}$ следует, что uv делится на δ. Поскольку $(uv) \mid \delta$ и $\delta \mid (uv)$, то $\delta = uv$.

В теории чисел доказываются теоремы о существовании первообразных корней по модулю p, по модулю p^k и по модулю $2p^k$, где p — простое нечетное число и k — произвольное положительное целое число.

Утверждение 1.8. Существуют первообразные корни по модулю p, где p — простое нечетное число.

Доказательство. Пусть $\delta_1, \delta_2, \ldots, \delta_k$ — все различные показатели, которым по модулю p принадлежат числа $1, 2, \ldots, (p-1)$. Пусть наименьшее общее кратное чисел $\delta_1, \delta_2, \ldots, \delta_k$ есть НОК$(\delta_1, \delta_2, \ldots, \delta_k) = \tau$, каноническое разложение которого имеет вид $\tau = {q_1}^{\alpha_1}{q_1}^{\alpha_2}\ldots{q_k}^{\alpha_k}$. Каждый множитель ${q_s}^{\alpha_s}$ этого разложения делит по меньшей мере один из показателей $\delta_1, \delta_2, \ldots, \delta_k$, например, число δ_j (это как раз тот показатель, который содержит множитель ${q_s}^{\alpha_s}$ и вносит его в разложение τ). Показатель δ_j можно записать в виде $\delta_j = z{q_s}^{\alpha_s}$. Пусть a_j — одно из чисел ряда $1, 2, \ldots, p-1$, принадлежащих показателю δ_j. Согласно утверждению 6, число $h_j = a_j^z$ принадлежит показателю ${q_s}^{\alpha_s}$. Поскольку показатели ${q_1}^{\alpha_1}$, ${q_1}^{\alpha_2}$, …, ${q_k}^{\alpha_k}$ являются попарно взаимно простыми, то, согласно утверждению 7, произведение $g = h_1h_2\ldots h_k$ принадлежит показателю ${q_1}^{\alpha_1}{q_1}^{\alpha_2}\ldots {q_k}^{\alpha_k} = \tau$. В соответствии со следствием к утверждению 5 показатель τ является делителем числа $p-1$: $\tau \mid (p-1)$.

Поскольку показатели $\delta_1, \delta_2, \ldots, \delta_k$, к каждому из которых относится хотя бы одно из чисел ряда $\{1, 2, \ldots, p-1\}$, делят τ, то все значения $1, 2, \ldots, (p-1)$ являются решениями сравнения $x^{\tau} \equiv 1 \bmod p$ *(см. утверждение 5)*. В теории чисел доказывается, что для простого p сравнение $a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0 \bmod p$ имеет не более n решений, если хотя бы один из коэффициентов $a_1, a_2, \ldots, a_n$ не кратен p. Из этого утверждения следует, что $p - 1 \le \tau$. Поскольку $\tau \mid (p-1)$ и $p - 1 \le \tau$, то $\tau = p - 1$. Следовательно, g является первообразным корнем по модулю p.

Таким образом, существуют первообразные корни по модулю простого числа. Этот факт учитывается при рассмотрении метода открытого распределения ключей Диффи-Хеллмана. Представляют интерес также следующие утверждения о существовании первообразных корней по модулям p^α и $2p^\alpha$, где p — нечетное простое число, которые мы приводим без доказательства.

Утверждение 1.9. Пусть g — первообразный корень по модулю простого числа p. Можно указать t с условием, что u, определяемое равенством $(g + pt)^{p-1} = 1 + pu$, не делится на p. Соответствующее $g + pt$ будет первообразным корнем по модулю p^α при любом $\alpha > 1$.

Утверждение 1.10. Пусть $\alpha \geq 1$ и g_1 — первообразный корень по модулю p^α, где p — нечетное простое число. Нечетное из чисел g' и $g' + p^\alpha$ будет первообразным корнем по модулю $2p^\alpha$.

Представляет интерес задача разыскивания первообразных корней по модулю p. Эта задача решается методом, использующим следующее утверждение.

Утверждение 1.11. Пусть $q_1, q_2, \ldots, q_k$ — различные простые делители функции Эйлера $\varphi(n)$ от числа n. Для того чтобы число g, взаимно простое с n, было первообразным корнем по модулю n, необходимо и достаточно, чтобы это g не удовлетворяло ни одному из сравнений:

$$g^{\varphi(n)/q_1} \equiv 1 \pmod{n},\ g^{\varphi(n)/q_2} \equiv 1 \pmod{n},\ \ldots,\ g^{\varphi(n)/q_k} \equiv 1 \pmod{n}.$$

1.5.2. Индексы по модулям p^α и $2p^\alpha$

По отношению к первообразным корням g вводится понятие индекса (при основании g) по модулю.

Утверждение 1.12. Пусть p — простое нечетное число, $\alpha \geq 1$; n — одно из чисел p^α и $2p^\alpha$; $c = \varphi(n)$, g — первообразный корень по модулю n. Если γ пробегает наименьшие неотрицательные вычеты $\gamma = 0, 1, \ldots, c-1$ по модулю c, то g^γ пробегает приведенную систему вычетов по модулю n.

Действительно, g относится к показателю c, и g^γ пробегает c чисел, взаимно простых с n, которые являются попарно несравнимыми по модулю n.

Для чисел a, взаимно простых с n, рассматривается понятие об индексе (дискретном логарифме), представляющее аналогию понятия о логарифме. Если $a \equiv g^\gamma \pmod{n}$ (предполагается, что $\gamma \geq 0$), то γ называется индексом числа a по модулю n при основании g и обозначается символом $\gamma = \operatorname{ind}_g a$ (или просто $\gamma = \operatorname{ind} a$). Из утверждения 1.12 следует, что всякое a, взаимно простое с n, имеет некоторый единственный индекс среди чисел ряда $\gamma = 0, 1, \ldots, c-1$. Зная γ', такое что $\gamma' = \operatorname{ind}_g a$, мы можем указать все индексы числа a: это будут все неотрицательные числа класса $\gamma \equiv \gamma' \pmod{c}$. Действительно, имеем $a \equiv g^\gamma \pmod{n}$ и $a \equiv g^{\gamma'} \pmod{n}$, поэтому $g^{\gamma - \gamma'} \equiv 1 \pmod{n}$, и поскольку g относится к показателю $c = \varphi(n)$, то $c \mid (\gamma - \gamma')$, т. е. $\gamma \equiv \gamma' \pmod{c}$.

Из определения индекса непосредственно следует, что числа с данным индексом γ образуют класс чисел по модулю n.

Рассмотрим следующие свойства индексов:

$$\mathrm{ind}_g\, ab\ldots l \equiv \mathrm{ind}_g\, a + \mathrm{ind}_g\, b + \ldots + \mathrm{ind}_g\, l \pmod{c}$$

и, в частности,

$$\mathrm{ind}_g\, a^n \equiv n\, \mathrm{ind}_g\, a \pmod{c}.$$

Действительно, перемножая сравнения $a \equiv g^{\mathrm{ind}\, a} \pmod{m}$, $b \equiv g^{\mathrm{ind}\, b} \pmod{m}$, …, $l \equiv g^{\mathrm{ind}\, l} \pmod{m}$, находим $ab\ldots l \equiv g^{\mathrm{ind}\, a + \mathrm{ind}\, b + \ldots + \mathrm{ind}\, l} \pmod{m}$. Следовательно, сумма $\mathrm{ind}_g\, a + \mathrm{ind}_g\, b + \ldots + \mathrm{ind}_g\, l$ является одним из индексов произведения $ab\ldots l$.

1.6. Теоремы о числе классов с заданным показателем

Рассмотрим вопрос о числе классов с заданным показателем. Иными словами, речь идет о количестве чисел, меньших модуля и относящихся к заданному показателю (каждое из таких чисел задает класс сравнимых с ним чисел по заданному модулю). Если взять классы, взаимно простые с модулем n, то каждый такой класс относится к некоторому показателю δ, причем $\delta \mid n$. Обозначим число классов, относящихся к показателю δ, через $\psi(\delta)$. Если δ не делит $\varphi(n)$, то такое δ не может быть показателем ни для какого числа, поэтому в данном случае имеем $\psi(\delta) = 0$. Если понятно, о каком модуле идет речь, то показатель числа a будем обозначать как $P(a)$.

Теорема 1.1. Сравнение степени k по простому модулю p с коэффициентом при старшем члене, не делящемся на p, может иметь не больше чем k решений.

Теорема 1.2. В последовательности $a, a^2, a^3, \ldots$ все числа принадлежат $P(a)$ классам, представителями которых являются числа $a, a^2, a^3, \ldots, a^{P(a)}$, где $P(a)$ есть показатель числа a по некоторому модулю n.

Доказательство. Числа $a, a^2, a^3, \ldots, a^{P(a)}$ попарно несравнимы по модулю n. Действительно, сравнение $a^i \equiv a^j \bmod n$ имеет место только тогда, когда $i \equiv j \bmod P(a)$. Но среди показателей степеней a в рассматриваемой последовательности нет сравнимых по модулю $P(a)$. С другой стороны, из сравнения $i \equiv j \bmod P(a)$ следует $a^i \equiv a^j \bmod n$, т. е. если показатели сравнимы по модулю $P(a)$, то степени сравнимы по модулю n. Поэтому в последовательности $a, a^2, a^3, \ldots$ не может быть больше чем $P(a)$ несравнимых между собой чисел, т. е. каждое число вида a^N сравнимо с некоторым числом из последовательности $a, a^2, a^3, \ldots, a^{P(a)}$.

Теорема 1.3. $P(a^i) = P(a)$ тогда и только тогда, когда НОД$(i, P(a)) = 1$.

Доказательство. *Достаточность*. Пусть НОД$(i, P(a)) = 1$. Найдем наименьшее положительное целое число δ, такое что $(a^i)^\delta \equiv 1 \bmod n$. Имеем $a^{i\delta} \equiv 1 \bmod n$, следовательно, $P(a) \mid i\delta$. Из условий НОД$(i, P(a)) = 1$ и $P(a) \mid i\delta$ следует, что $P(a) \mid \delta$ и наименьшее натуральное число, делящееся нацело на $P(a)$, равно $\delta = P(a)$.

Необходимость. Предположим противное: НОД$(i, P(a)) = d > 1$. Тогда $\dfrac{P(a)}{d}$ и $\dfrac{i}{d}$ являются целыми числами и $(a^i)^{\frac{P(a)}{d}} = (a^{P(a)})^{\frac{i}{d}} \equiv 1 \bmod n$, т. е. $P(a^i) \le \dfrac{P(a)}{d} < P(a)$.

Эта теорема показывает, что среди степеней последовательности $a, a^2, a^3, \ldots, a^{P(a)}$ все степени a^i, у которых i взаимно простое с $P(a)$, имеют тот же показатель по модулю n, что и само число a.

Теорема 1.4. Если по модулю n $P(a) = k$, то классы $\overline{a}, \overline{a^2}, \ldots, \overline{a^k}$ представляют собой различные решения сравнения $x^k \equiv 1 \bmod n$. (В общем случае указанные классы не охватывают *всех* решений данного сравнения.)

Доказательство. Если $P(a) = k$, то $a^k \equiv 1 \bmod n$, поэтому при произвольном значении целого числа $i \geq 0$ имеем $(a^i)^k = (a^k)^i \equiv 1 \bmod n$. Поэтому все числа a^i удовлетворяют сравнению $x^k \equiv 1 \bmod n$, т. е. классы $\overline{a}, \overline{a^2}, \ldots, \overline{a^k}$ есть решения этого сравнения. Согласно теореме 1.2, все эти решения различны. Но в общем случае существуют и другие решения, например, для такого составного модуля n, при котором $P(a) = L(n)$, решениями сравнения $x^{P(a)} \equiv 1 \bmod n$ являются классы $\overline{1}, \overline{2}, \ldots, \overline{n-1}$, тогда как теорема указывает на $L(n) < n - 1$ решений.

Теорема 1.5. Если по простому модулю p $P(a) = k$, то классы $\overline{a}, \overline{a^2}, \ldots, \overline{a^k}$ представляют собой *все* решения сравнения $x^k \equiv 1 \bmod p$.

Доказательство. В теореме 4 установлено, что классы $\overline{a}, \overline{a^2}, \ldots, \overline{a^k}$ образуют различные решения сравнения $x^k \equiv 1 \bmod n$. Поскольку p есть простой модуль, то это сравнение не может иметь больше чем k решений (теорема 1), т. е. классы $\overline{a}, \overline{a^2}, \ldots, \overline{a^k}$ исчерпывают все решения.

Теорема 1.6. Количество классов, относящихся к какому-либо показателю по модулю n, равно функции Эйлера $\varphi(n)$ от модуля:

$$\sum_{\delta|\varphi(n)} \psi(\delta) = \varphi(n).$$

Доказательство. Доказательство непосредственно следует из того, что каждый из взаимно простых с модулем классов относится к какому-либо показателю.

Теорема 1.7. По простому модулю p для любого целого $\delta \geq 1$ имеет место неравенство $\psi(\delta) \leq \varphi(\delta)$.

Доказательство. Если для данного значения показателя δ не существует классов, относящихся к нему, то $\psi(\delta) = 0$, т. е. $\psi(\delta) < \varphi(\delta)$. Если существует хоть один такой класс $\overline{a}$, то классы, к которым относятся числа $a, a^2 \bmod p, a^3 \bmod p, \ldots, a^\delta \bmod p$, образуют все решения сравнения $x^\delta \equiv 1 \bmod p$. По теореме 1.3 $P(a^i) = P(a)$, $1 \leq i \leq \delta$ тогда и только тогда, когда НОД$(P(a), i) = 1$. Число таких степеней i равно $\varphi(\delta)$. Если имеется какой-либо класс, показатель которого по модулю p равен δ, то он также должен удовлетворять сравнению $x^\delta \equiv 1 \bmod p$. Поэтому класс должен находиться среди $\varphi(\delta)$ классов, представителями которых являются числа $a, a^2 \bmod p, a^3 \bmod p, \ldots, a^\delta \bmod p$. Отсюда следует, что $\psi(\delta) = \varphi(p)$, если $\psi(\delta) \neq 0$. Учитывая случай $\psi(\delta) = 0$, имеем $\psi(\delta) \leq \varphi(\delta)$.

Теорема 1.8. По простому модулю p при $\delta \mid p-1$ имеет место равенство $\psi(\delta) = \varphi(\delta)$.

Теорема 1.9. По любому простому модулю p существует $\varphi(p-1)$ первообразных корней.

Доказательство. Доказательство вытекает непосредственно из теоремы 1.8 при $\delta = p-1$.

Теорема 1.10. Первообразные корни по модулю n существуют тогда и только тогда, когда: либо 1) $n = p^{\alpha}$ или $n = 2p^{\alpha}$, где p — любое нечетное простое число, α — любое целое положительное число; либо 2) $n = 2^{\alpha}$, где $0 \le \alpha \le 2$.

Пояснение. Если n имеет хотя бы два нечетных простых делителя p_1 и p_2, то числа $p_1 - 1$ и $p_2 - 1$ не являются взаимно простыми, поэтому $L(n) < \varphi(n)$. Из обобщенной теоремы Эйлера следует, что для любого a, взаимно простого с n, имеем $P(a) \le L(n) < \varphi(n)$, т. е. первообразных корней не существует.

1.7. Китайская теорема об остатках

Эта теорема является одним из весьма полезных и часто используемых в криптографии результатов теории чисел. Она фактически утверждает, что любое значение из множества минимальных положительных представителей ($\mathbb{Z}/N$) классов вычетов по модулю $N = n_1 n_2 \ldots n_g$, где $\forall\, i, j \in \{1, 2, \ldots, g\}$ НОД$(n_i, n_j) = 1$, может быть представлено в виде набора остатков от деления этого значения на каждый из сомножителей n_i; т. е. имеется взаимно однозначное соответствие

$$R \leftrightarrow (r_1, r_2, \ldots, r_g), \text{ где } R \in \mathbb{Z}/N,\ r_1 \in \mathbb{Z}/n_1,\ r_2 \in \mathbb{Z}/n_2,\ \ldots,\ r_g \in \mathbb{Z}/n_g.$$

Китайская теорема об остатках гласит следующее.

Теорема 1.11. Пусть $n_1, n_2, \ldots, n_g$ — набор попарно взаимно простых чисел, $N = n_1 n_2 \ldots n_g$; числа $c_1, c_2, \ldots, c_g$ удовлетворяют условиям $c_1 N/n_1 \equiv 1 \bmod n_1$, $c_2 N/n_2 \equiv 1 \bmod n_2$, …, $c_g N/n_g \equiv 1 \bmod n_g$. Тогда решение системы

$$\begin{cases} x \equiv r_1 \bmod n_1 \\ x \equiv r_2 \bmod n_2 \\ \quad \ldots\ldots \\ x \equiv r_g \bmod n_g \end{cases}$$

имеет вид $R' \equiv r_1 c_1 N/n_1 + r_2 c_2 N/n_2 + \ldots + r_g c_g N/n_g \pmod N$.

Доказательство. Поскольку $\forall\, i, j \in \{1, 2, \ldots, g\}$ и $i \ne j$ $n_i \left| \frac{N}{n_j} \right.$ (например $n_1 \left| \frac{N}{n_2} \right.$, $n_3 \left| \frac{N}{n_2} \right.$, …, $n_g \left| \frac{N}{n_2} \right.$), то $R' \bmod n_i = (r_1 c_1 N/n_1 + r_2 c_2 N/n_2 + \ldots + r_g c_g N/n_g) \bmod n_i =$ $= (r_i c_i N/n_i) \bmod n_i$. То есть $R' \equiv r_i c_i N/n_i \equiv r_i \pmod{n_i}$ для $i = 1, 2, \ldots, g$.

Минимальное положительное число R из класса вычетов по модулю N, представляющего собой решение системы сравнений, и является тем элементом кольца $\mathbb{Z}/N$,

который ставится в соответствие набору значений $r_1, r_2, \ldots, r_g$. Подобрать необходимые значения $c_iN/n_i \equiv 1 \bmod n_i$ достаточно просто. Их можно вычислить по формуле $c_iN/n_i = [(n_i/N) \bmod n_i]N/n_i$. Если дано некоторое $R \in \mathbb{Z}/N$, то, выполнив деление R на каждое из чисел n_i, определим однозначно набор остатков, который ставится в соответствие заданному числу R. Фактически китайская теорема об остатках указывает способ решения сравнений указанного типа.

В дальнейшем будет использована также следующая теорема.

Теорема 1.12. Если $a \equiv b \pmod{n_1}$, $a \equiv b \pmod{n_2}$,…, $a \equiv b \pmod{n_g}$, то $a \equiv b \pmod{N}$, где $N = \text{НОК}[n_1, n_2, \ldots, n_g]$.

Доказательство. Из условия непосредственно следует, что $n_1 \mid a - b$, $n_2 \mid a - b$, …, $n_g \mid a - b$, откуда получаем $N \mid a - b$. Последнее означает, что выполняется $a \equiv b \pmod{N}$.

1.8. Теоремы о числе решений степенных сравнений

Вначале рассмотрим несколько утверждений, используемых далее при доказательстве теорем о числе решений степенных сравнений.

Утверждение 1.13. Для произвольных натуральных чисел k и m из выполнимости сравнения $a \equiv b \pmod{m}$ следует сравнимость чисел ka и kb по модулю km, т. е. $ka \equiv kb \pmod{km}$.

Доказательство. По условию имеем $k > 0$ и $m \mid a - b$, откуда следует $km \mid ka - kb \Rightarrow ka \equiv kb \pmod{km}$.

Утверждение 1.14. Для произвольных натуральных чисел k и m из выполнимости сравнения $ka \equiv kb \pmod{km}$ следует сравнимость чисел a и b по модулю m, т. е. $a \equiv b \pmod{m}$.

Доказательство. По условию имеем $k \neq 0$ и $km \mid ka - kb$, откуда следует $km \mid k(a - b) \Rightarrow m \mid a - b \Rightarrow a \equiv b \pmod{km}$.

Утверждение 1.15. Если обе части сравнения $f(x) \equiv g(x) \pmod{m}$ и модуль умножим на одно и то же число $k > 0$, то получим сравнение $kf(x) \equiv kg(x) \pmod{km}$, эквивалентное первоначальному.

Доказательство. Если при некотором $x = x_0$ имеем $f(x_0) \equiv g(x_0) \pmod{m}$, то из утверждения 1.13 имеем $kf(x_0) \equiv kg(x_0) \pmod{km}$. Из $kf(x_0) \equiv kg(x_0) \pmod{km}$, согласно утверждению 1.14, имеем $f(x_0) \equiv g(x_0) \pmod{m}$.

Утверждение 1.16. Если НОД$(a, m) = d$ и $d \nmid b$, то сравнение $ax \equiv b \pmod{m}$ не имеет решений.

Доказательство. Допустим, что существует число x_0, такое что $ax_0 \equiv b \pmod{m}$, т. е. $ax_0 = Qm + b$, где Q есть некоторое целое число. Поскольку $d \mid ax_0$ и $d \mid m$, то из последнего равенства следует $d \mid b$. Мы пришли к противоречию, следовательно, наше допущение неверно, что доказывает утверждение.

Утверждение 1.17. Если НОД(a, m) = 1, то сравнение $ax \equiv b \pmod m$ имеет единственное решение.

Доказательство. Если НОД(a, m) = 1, то в приведенной системе наименьших неотрицательных вычетов по модулю m существует единственный элемент a^{-1}, такой что $a^{-1}a = 1$. Для этого элемента имеем НОД(a^{-1}, m) = 1. Умножая обе части сравнения $ax \equiv b \pmod m$ на a^{-1}, получим $a^{-1}ax \equiv a^{-1}b \pmod m \Rightarrow x \equiv a^{-1}b \pmod m$.

Утверждение 1.18. Числа класса $\overline{a}$ по модулю m образуют следующие k классов по модулю km : $\overline{a}, \overline{a+m}, \overline{a+2m}, \ldots, \overline{a+(k-1)m}$.

Утверждение 1.19. Если НОД(a, m) = d и $d \mid b$, то сравнение $ax \equiv b \pmod m$ имеет d решений. Все эти решения принадлежат одному классу по модулю m/d.

Доказательство. Из утверждения 1.15 следует, что при НОД(a, m) = d и $d \mid b$ сравнение $ax \equiv b \pmod m$ эквивалентно сравнению вида $a_1x \equiv b_1 \pmod{m_1}$, где $m_1 = m/d$, НОД(a_1, m_1) = 1.

Согласно утверждению 1.17, последнее сравнение имеет одно решение, представляющее собой один класс по модулю m/d, т. е. этому сравнению удовлетворяют числа вида $x \equiv \alpha \pmod{m/d}$, где α может быть найдено, например, по формуле $x \equiv a_1^{-1}b_1 \equiv a_1^{\varphi(m/d)-1}b_1 \pmod{m/d}$. Числа этого класса по модулю m/d образуют d классов по модулю m *(см. утверждение 1.18)*, и решения сравнения $ax \equiv b \pmod m$ могут быть записаны в виде $x \equiv \alpha \pmod m$, $x \equiv \alpha + m/d \pmod m$, …, $x \equiv \alpha + (d-1)m/d \pmod m$.

Утверждение 1.20. Если НОД(a, m) = 1 и x пробегает значения, образующие приведенную систему вычетов, то ax также принимает значения, образующие приведенную систему вычетов по модулю m.

Теорема 1.13.

1. При $p \nmid a$ сравнение $x^n \equiv a \pmod p$ по простому модулю $p > 2$ либо совсем не имеет решений, либо число решений равно наибольшему общему делителю n и $p-1$.

2. Сравнение (1) не имеет решений, если для δ = НОД(n, $p-1$) $\delta \nmid \operatorname{ind} a$, и имеет δ решений, если $\delta \mid \operatorname{ind} a$.

Доказательство. Пусть НОД(n, $p-1$) = δ. По простому модулю p существуют первообразные корни *(см. утверждение 1.8)*. Пусть g есть некоторый первообразный корень. Индексируя сравнение

$$x^n \equiv a \pmod p \tag{1.1}$$

по основанию g, получаем сравнение

$$n \operatorname{ind} x \equiv \operatorname{ind} a \pmod{p-1}, \tag{1.2}$$

которое эквивалентно исходному. Если обозначить $\operatorname{ind} x = z$, $\operatorname{ind} a = b$, то для неизвестной z получим сравнение 1-й степени:

$$nz \equiv b \pmod{p-1}. \tag{1.3}$$

При $\delta \nmid \operatorname{ind} a$, т. е. $\delta \nmid b$, сравнение (1.3) не имеет решений *(см. утверждение 1.16)*, но тогда не существует и значений x, удовлетворяющих сравнениям (1.2) и (1.1). При $\delta \mid \operatorname{ind} a$, т. е. $\delta \mid b$, согласно утверждению 1.19, сравнение (1.3) имеет δ решений. Значения $\operatorname{ind} x$, удовлетворяющие сравнению (1.2), принадлежат δ классам по модулю $p-1$, а следовательно, и для x существует δ классов по модулю p, удовлетворяющих сравнению (1.1).

Замечание

1. При $p \mid a$ сравнение (1.1) может быть записано в виде $x^n \equiv 0 \pmod p$, и в этом случае оно имеет одно решение $x \equiv 0 \pmod p$.
2. Пусть g и h — произвольные первообразные корни по модулю p. Тогда имеем

$$h \equiv g^{\operatorname{ind}_g h} \equiv (h^{\operatorname{ind}_h g})^{\operatorname{ind}_g h} \equiv h^{\operatorname{ind}_h g \cdot \operatorname{ind}_g h} \pmod p \Rightarrow \operatorname{ind}_h g \cdot \operatorname{ind}_g h \equiv 1 \pmod{p-1} \Rightarrow$$

$$\Rightarrow \operatorname{ind}_h g \equiv (\operatorname{ind}_g h)^{-1} \pmod{p-1},$$

   т. е. индексы первообразных корней являются взаимно простыми с $p-1$. Действительно, пусть $\text{НОД}(\operatorname{ind}_g a, p-1) = \delta > 1$. Тогда

$$a^{\frac{p-1}{\delta}} \equiv (g^{\operatorname{ind}_g a})^{\frac{p-1}{\delta}} \equiv (g^{p-1})^{\frac{\operatorname{ind}_g a}{\delta}} \equiv 1^z \equiv 1 \pmod p,$$

   где z — целое число, т. е. показатель, к которому относится число a, меньше чем $p-1$. Поскольку $\text{НОД}(\operatorname{ind}_h g, p-1) = 1$ и $\operatorname{ind}_h a \equiv \operatorname{ind}_h g \cdot \operatorname{ind}_g a$, то из $\delta \nmid \operatorname{ind}_g a$ (или из $\delta \mid \operatorname{ind}_g a$) следует $\delta \nmid \operatorname{ind}_h a$ (или $\delta \mid \operatorname{ind}_h a$).
3. Заметим, что $\operatorname{ind} 1 = p-1$, т. е. $\operatorname{ind} 1 \equiv 0 \pmod{p-1}$. Следовательно, $\delta \mid \operatorname{ind} 1$ и сравнение $x^n \equiv 1 \pmod p$ имеет δ решений.

Определение.

1. Число a называется вычетом n-й степени по простому модулю p, если $p \nmid a$ и сравнение $x^n \equiv a \pmod p$ имеет решения.

2. Число a называется невычетом n-й степени по простому модулю p, если сравнение $x^n \equiv a \pmod p$ не имеет решений.

Теорема 1.14. По простому модулю $p > 2$ число классов вычетов n-й степени равно $(p-1)/\delta$, где $\delta = \text{НОД}(n, p-1)$.

Доказательство. Всего по модулю p имеется $p-1$ классов, взаимно простых с модулем (класс $\overline{0}$, состоящий из чисел, делящихся на p, согласно указанному ранее определению, не относится к вычетам n-й степени). Индексы этих классов образуют полную систему вычетов по модулю $p-1$, т. е. каждому такому классу (если взять $\operatorname{ind} 1 = p-1$) можно сопоставить индекс, равный одному из чисел: $1, 2, \ldots, p-1$.

Пусть $\text{НОД}(n, p-1) = \delta$. Среди чисел $1, 2, \ldots, p-1$ имеется $\dfrac{p-1}{\delta}$ чисел, делящихся на δ, которыми являются числа $\delta, 2\delta, \ldots, (\dfrac{p-1}{\delta} - 1)\delta$, $(p-1)$. Эти числа являются индексами $\dfrac{p-1}{\delta}$ различных чисел из множества $\{1, 2, \ldots, p-1\}$. Если a равно лю-

бому из этих чисел, то, согласно теореме 1.13, сравнение $x^n \equiv a \pmod p$ имеет решения, т. е. существует $\frac{p-1}{\delta}$ классов вычетов n-й степени по простому модулю p.

Теорема 1.15. Если $\delta = \text{НОД}(n, p-1)$, то вычеты n-й степени по простому модулю $p > 2$ совпадают с вычетами степени δ по этому модулю.

Доказательство. Если $\text{НОД}(n, p-1) = \delta$, то будем иметь также $\text{НОД}(\delta, p-1) = \delta$. При $p \nmid a$ сравнения $x^n \equiv a \pmod p$ и $x^\delta \equiv a \pmod p$, согласно теореме 1.13, имеют решения при одних и тех же числах a, таких что $\delta \mid \text{ind}\, a$.

В силу теоремы 1.15 можно рассматривать вычеты и невычеты n-й степени только для таких n, которые являются делителями числа $p-1$, т. е. рассматривать сравнения вида $x^n \equiv a \pmod p$, где $n \mid p-1$. Действительно, сравнение $x^n \equiv a \pmod p$ можно записать в виде:

$$(x^\delta)^{n/\delta} \equiv a \pmod p, \tag{1.4}$$

где $\text{НОД}((n/\delta), p-1) = 1$, т. е. сравнение (1.4) имеет единственное решение относительно неизвестной $z = x^\delta$. Пусть $x^\delta \equiv b \pmod p$. Последнее сравнение имеет вид сравнения $x^n \equiv a \pmod p$, где $n \mid p-1$. Для случая $n \mid p-1$ теоремы 1.13 и 1.14 имеют следующую формулировку.

Теорема 1.13*. При $p \nmid a$ и $n \mid p-1$ сравнение $x^n \equiv a \pmod p$ по простому модулю $p > 2$ либо совсем не имеет решений, либо имеет n решений. По такому модулю a является вычетом n-й степени тогда и только тогда, когда $n \mid \text{ind}\, a$.

Теорема 1.14*. По простому модулю $p > 2$ и $n \mid p-1$ число классов вычетов n-й степени равно $(p-1)/n$.

Теорема 1.16. При $n \mid p-1$ a является вычетом n-й степени по простому модулю $p > 2$ тогда и только тогда, когда $a^{(p-1)/n} \equiv 1 \pmod p$.

Доказательство. Индексируя сравнение $a^{(p-1)/n} \equiv 1 \pmod p$, получаем, что это сравнение имеет место тогда и только тогда, когда $\frac{p-1}{n}\text{ind}\, a \equiv 0 \pmod{p-1}$, т. е. когда $\frac{p-1}{n}\text{ind}\, a = Q(p-1)$ или $\text{ind}\, a = nQ$ (Q — целое число), т. е. сравнение $a^{(p-1)/n} \equiv 1 \pmod p$ имеет место тогда и только тогда, когда $n \mid \text{ind}\, a$.

Теорема 1.17. При $p \nmid a$ и $n \mid p-1$ все решения сравнения $x^n \equiv a \pmod p$ по простому модулю $p > 2$ можно получить, умножая одно решение этого сравнения на различные решения сравнения $x^n \equiv 1 \pmod p$.

Другими словами, все корни n-й степени из $\bar{a}$ по модулю p можно получить, умножая один из этих корней на различные корни n-й степени из $\bar{1}$

Доказательство. Поскольку $\text{ind}\, 1 = 0$ и $n \mid 0$, сравнение $x^n \equiv 1 \pmod p$ имеет n решений. Обозначим эти решения через $\bar{t}_1, \ldots, \bar{t}_n$, где $t_i \not\equiv t_j \pmod p$ и $p \nmid t_i$. Пусть $\overline{x_0}$ удовлетворяет сравнению (1.1), тогда $(x_0 t_i)^n = x_0^n t_i^n \equiv a \cdot 1 \equiv a \pmod p$ при $i = 1,$

2, …, n, т. е. классы $\overline{x_0 t_1}, \ldots, \overline{x_0 t_n}$ представляют собой решения сравнения $x^n \equiv a \pmod p$.

Поскольку $p \nmid a$, то $p \nmid x_0$ и НОД(x_0, p) = 1, следовательно, числа $x_0 t_1$, …, $x_0 t_n$ являются (утверждение 1.20) частью приведенной системы вычетов по модулю p и $x_0 t_1$, …, $x_0 t_n$ представляют собой n различных решений сравнения (1.1). Степень этого сравнения равна n, следовательно, $x_0 t_1$, …, $x_0 t_n$ охватывают все решения.

Важным частным случаем степенных сравнений являются сравнения второй степени. Из доказанных ранее теорем вытекают следующие следствия, относящиеся к случаю $n = 2$.

Следствие 1.3. Необходимым и достаточным условием того, чтобы число a было квадратичным вычетом по простому модулю $p > 2$ ($p \nmid a$), является выполнимость сравнения

$$a^{\frac{p-1}{2}} \equiv 1 \pmod p.$$

Следствие 1.4. Если a является квадратичным вычетом по простому модулю $p > 2$ ($p \nmid a$), то сравнение $x^2 \equiv a \pmod p$ имеет два решения.

Следствие 1.5. По любому простому модулю $p > 2$ ($p \nmid a$) число классов квадратичных вычетов и число классов квадратичных невычетов равно $\frac{p-1}{2}$.

Для сравнений $x^2 \equiv a \pmod p$ имеет место следующее утверждение.

Теорема 1.18. Необходимым и достаточным условием того, чтобы число a было квадратичным невычетом по простому модулю $p > 2$ ($p \nmid a$), является выполнимость сравнения $a^{\frac{p-1}{2}} \equiv -1 \pmod p$.

Доказательство. В силу малой теоремы Ферма имеем $a^{p-1} - 1 \equiv 0 \pmod p$. Поскольку $2 \mid p - 1$, то можем записать $(a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) \equiv 0 \pmod p$. Последнее сравнение выполняется, когда имеет место либо $a^{\frac{p-1}{2}} - 1 \equiv 0 \pmod p$, либо $a^{\frac{p-1}{2}} + 1 \equiv 0 \pmod p$. Первое из последних двух сравнений выполняется, когда a является квадратичным вычетом. Если a является квадратичным невычетом, то имеем $a^{\frac{p-1}{2}} + 1 \equiv 0 \pmod p$.

Глава 2

Алгоритмы двухключевой криптографии

2.1. Генерация простых чисел

Для генерации больших простых чисел могут быть использованы следующие два подхода:

- формируются случайные числа заданного размера и проверяется, являются ли они простыми, с помощью вероятностных тестов (псевдопростые числа);
- по определенной процедуре генерируются простые числа, проверка которых осуществляется с помощью детерминистических тестов на простоту.

В первом случае тесты строятся на основе определенных теорем из теории чисел, сформулированных и доказанных для простых чисел. Если число не удовлетворяет тесту, то оно не является простым и отбрасывается. Для проверки берется следующее случайное число требуемого размера. Если число проходит тест, то некоторый переменный параметр, используемый для тестирования, изменяется и тест повторяется снова. Число, прошедшее большое число опытов определенного типа, считается *псевдопростым*, поскольку вероятность, что составное число может пройти все тесты, пренебрежимо мала. Для того чтобы исключить некоторые возможные классы составных чисел, которые могут проходить тесты конкретного типа, используют несколько различных тестов, по каждому из которых выполняется большое число опытов. Достоинством генерации псевдопростых чисел является сравнительная простота процедуры. Недостатком первого подхода является то, что после генерации большого псевдопростого числа p может оказаться достаточно сложным определение разложения числа $p-1$, которое необходимо знать, например, в случае ЭЦП на основе сложности задачи дискретного логарифмирования с сокращенной длиной подписи. Разложение числа $p-1$ представляет интерес также и для отсеивания некоторых классов слабых простых чисел. Следующие два вероятностных теста могут быть применены совместно. Пусть мы хотим проверить, является ли число p простым.

- *Тест Ферма* заключается в проверке соотношения $b^{p-1} = 1 \pmod{p}$ для большого числа различных значений b. Число различных использованных при тестировании значений b, для которых выполняется указанное соотношение, определяет число выполненных опытов по тесту Ферма. Однако известен класс составных

чисел, которые проходят тест Ферма (числа Кармайкла; например $1105 = 5 \cdot 13 \cdot 17$ и $41041 = 7 \cdot 11 \cdot 13 \cdot 41$).

- *Тест Соловея — Штрассена* заключается в проверке равенства $b^{\frac{p-1}{2}} \bmod \left(\frac{b}{p}\right)$, где $\left(\frac{b}{p}\right)$ — символ Лежандра, $\left(\frac{b}{p}\right) = 1$ для значений b, являющихся квадратичными вычетами по модулю p, и $\left(\frac{b}{p}\right) = -1$ для значений b, являющихся квадратичными невычетами по модулю p (квадратичным вычетом называется число, являющееся квадратом некоторого числа x по модулю p; т. е. для квадратичного вычета существует квадратный корень: $b = x^2 \bmod p$).

Второй тест хорошо отсеивает числа Кармайкла. Вероятность того, что составное число пройдет один опыт по тесту Соловея — Штрассена, не превышает значения 0,5. Это позволяет получить оценку числа опытов, которые следует выполнить в соответствии с данным тестом, чтобы получить необходимо низкую вероятность принятия составного числа в качестве псевдопростого. Первый тест используется в качестве предварительной отбраковки чисел. Второму тесту подвергают только числа, прошедшие первый. (Второй тест на самом деле поглощает первый, поскольку проверка условия $b^{\frac{p-1}{2}} \bmod p = 1$ для значений b, являющихся квадратичными вычетами, фактически означает проверку по тесту Ферма.)

2.2. Детерминистическая генерация больших простых чисел

2.2.1. Способ на основе подбора разложения функции Эйлера

Формируется набор k простых чисел $\{q_1, q_2, \ldots, q_k\}$ сравнительно малой длины (например, имеющих 8—10 десятичных знаков). Причем числа $q_1, q_2, \ldots, q_k$ проверяются детерминистическим тестом на простоту, в качестве которого можно взять проверку на делимость на все натуральные числа от 2 до $\lceil \sqrt{q_i} \rceil$ (метод пробного деления; $\lceil g \rceil$ обозначает наименьшее целое число, не меньшее, чем число g). Из указанного набора случайным образом выбираются h простых чисел $m_1, m_2, \ldots, m_h$, вычисляется число p_1, имеющее следующую структуру:

$$p_1 = 1 + 2\prod_{i=1}^{i=h} m_i.$$