Н. А. Молдовян

ПРАКТИКУМ ПО КРИПТОСИСТЕМАМ С ОТКРЫТЫМ КЛЮЧОМ

- *Математический минимум*
- *Алгоритмы электронной цифровой подписи*
- *Новые схемы ЭЦП*
- *Задачи с решениями по анализу и синтезу ЭЦП*
- *Задания для курсовых работ*

УЧЕБНОЕ ПОСОБИЕ

bhv®

Н. А. Молдовян

ПРАКТИКУМ ПО КРИПТОСИСТЕМАМ С ОТКРЫТЫМ КЛЮЧОМ

Санкт-Петербург
«БХВ-Петербург»
2014

УДК 681.3
ББК 32.81
М75

Молдовян Н. А.

М75 Практикум по криптосистемам с открытым ключом. — СПб.: БХВ-Петербург, 2014. — 304 с.: ил.

ISBN 5-9775-0024-6

Приведено краткое изложение математических результатов, используемых при синтезе и анализе криптосистем с открытым ключом, и ряда классических и новых криптосистем этого типа, включая достаточно большое число схем электронной цифровой подписи (ЭЦП). Основная часть книги содержит материалы для проведения практических занятий: формулировки заданий для курсовых работ и проектов и большое количество оригинальных задач, связанных с новыми схемами ЭЦП или вопросами, касающимися синтеза и анализа последних. Все задачи сопровождаются подробными указаниями и решениями.

Для преподавателей, студентов и аспирантов инженерно-технических вузов

УДК 681.3
ББК 32.81

Группа подготовки издания:

Главный редактор	*Екатерина Кондукова*
Зам. главного редактора	*Игорь Шишигин*
Зав. редакцией	*Григорий Добин*
Компьютерная верстка	*Сергея Матвеева*
Корректор	*Наталия Першакова*
Дизайн обложки	*Игоря Цырульникова*
Зав. производством	*Николай Тверских*

Формат 70×100 1/16. Усл. печ. л. 24,51. Доп. тираж 40 экз.
"БХВ-Петербург", 191036, Санкт-Петербург, Гончарная ул., 20.

Отпечатано в цифровой типографии "Галерея печати "ИПК НП-Принт"
190005, Санкт-Петербург, Измайловский пр., 29.

ISBN 5-9775-0024-6

Содержание

Введение

В настоящее время проблематика и методы криптографии входят в ряд курсов по подготовке специалистов в области защиты информации и информационных технологий в целом. К настоящему моменту появилось достаточно большое число книг на русском языке, затрагивающих вопросы классической и современной криптографии. Среди этих книг имеются справочники, монографии, учебные пособия и учебники, написанные зарубежными и российскими авторами. Благодаря этому студенты, аспиранты и молодые специалисты имеют достаточно широкие возможности по выбору теоретического материала, однако материал для практических занятий в имеющихся книгах проработан недостаточно. В частности, отсутствует материал для подготовки заданий к курсовым работам и проектам, а приводимые для самопроверки вопросы и задачи не снабжены достаточно подробными указаниями и решениями. Целью данной книги является восполнение этого пробела по отношению к криптосистемам с открытым ключом. Она является дополнением к учебному пособию Н. А. Молдовяна и А. А. Молдовяна «Введение в криптосистемы с открытым ключом» (БХВ-Петербург, 2005) и включает следующий материал:

- краткий перечень основных понятий и результатов теории чисел, используемых при построении и анализе двухключевых криптосистем;
- краткий обзор классических криптосистем с открытым ключом;
- алгоритмический минимум, дающий возможность получить представление, как организуются вычисления в двухключевых криптосистемах;
- описание некоторых новых систем с открытым ключом, расширяющих набор конструктивных механизмов, которые использованы для разработки вариантов курсовых заданий и при составлении задач;
- около 200 вариантов заданий для выполнения курсовых работ и проектов;

- список задач по элементам теории чисел, необходимым для понимания вычислительных процедур, лежащих в основе криптосистем с открытым ключом;
- список задач по двухключевой криптографии, который, в частности, охватывает тематику анализа и синтеза систем электронной цифровой подписи различного типа;
- решения, указания и ответы ко всем задачам, число которых составляет около 300.

При этом преобладающую часть объема книги занимает рассмотрение курсовых заданий и задач.

Данное учебное пособие ориентировано в первую очередь на студентов и преподавателей вузов, аспирантов и молодых специалистов, работа и исследования которых затрагивают вопросы криптографии.

ГЛАВА 1

Понятия и результаты теории чисел

Более полно с результатами теории чисел и их доказательствами можно ознакомиться в работах [1, 2, 3].

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.

Взаимно простыми называются два целых положительных числа, наибольший общий делитель которых равен 1.

1.1. Сравнения: некоторые свойства и теоремы

Два числа a и b называются сравнимыми по некоторому модулю n, если разность $a-b$ делится на n без остатка. Сравнимость можно определить также и следующим образом: два числа a и b называются сравнимыми по некоторому модулю n, если остатки от деления a на n и b на n равны между собой. Если принять второе определение, то первое является следствием, и наоборот.

Утверждение 1

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

Утверждение 2

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

Следствие 1

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

Утверждение 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 эффективно вычислять наибольший общий делитель (НОД) двух натуральных чисел.

Теорема Ферма

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

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

Функция Эйлера обозначается символом $\varphi(n)$ и определяется как число положительных целых чисел, которые меньше натурального числа $n > 1$ и являются взаимно простыми с n. По определению $\varphi(1) = 1$. Функция Эйлера является мультипликативной функцией, т. е. для двух взаимно простых чисел a и b выполняется соотношение $\varphi(ab) = \varphi(a) \times \varphi(b)$. Произвольное число n может быть представлено в виде произведения, содержащего только взаимно простые сомножители вида p^s, где $s \geq 1$ и p — простое число. Для числа p^s имеем:

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

Теорема Эйлера

Для любых взаимно простых чисел a и n выполняется сравнение

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

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

1.2. Показатели и первообразные корни

Определение

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

Утверждение 4

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

Утверждение 5

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

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

Следствие 2

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

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

Утверждение 6

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

Утверждение 7

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

Интересен вопрос о существовании чисел, принадлежащих показателю $\varphi(n)$. Такие числа существуют и называются первообразными корнями по модулю n. 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 8

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

Утверждение 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 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 $2p^{\alpha}$.

Утверждение 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:

$$g^{c/q_1} \equiv 1 \bmod n,\ g^{c/q_2} \equiv 1 \bmod n,\ \ldots,\ g^{c/q_k} \equiv 1 \bmod n.$$

1.3. Индексы по модулям p^{α} и $2p^{\alpha}$

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

Утверждение 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.

Для чисел a, взаимно простых с n, рассматривается понятие об индексе (дискретном логарифме), представляющее аналогию понятия о логарифме. Если $a \equiv g^{\gamma} \bmod n$ (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 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 $\gamma \equiv \gamma' \bmod c$. Действительно, имеем $a \equiv g^{\gamma} \bmod n$ и $a \equiv g^{\gamma'} \bmod n$, поэтому $g^{\gamma - \gamma'} \equiv 1 \bmod n$, и поскольку g относится к показателю $c = \varphi(n)$, то $c \mid (\gamma - \gamma')$, т. е. $\gamma \equiv \gamma' \bmod c$.

Из определения индекса непосредственно следует, что числа с данным индексом γ образуют класс чисел по модулю n. Индексы обладают следующими свойствами:

$$\operatorname{ind}_g ab\ldots l \equiv \operatorname{ind}_g a + \operatorname{ind}_g b + \ldots + \operatorname{ind}_g l \pmod c,\ \operatorname{ind}_g a^n \equiv n \operatorname{ind}_g a \pmod c.$$

1.4. Теоремы о числе классов с заданным показателем

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 этом случае имеем $\psi(\delta) = 0$. Показатель числа a будем обозначать как $P(a)$.

Теорема 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 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.

Теорема 3

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

Теорема 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.)

Теорема 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 $x^k \equiv 1 \bmod p$.

Теорема 6

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

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

Теорема 7

По простому модулю p для любого целого $\delta \geq 1$ имеет место неравенство

$$\psi(\delta) \leq \varphi(\delta).$$

Теорема 8

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

Теорема 9

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

Теорема 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 $0 \le \alpha \le 2$.

Теорема 11

$$\sum_{\forall d|m} \varphi(d) = m.$$

Теорема 6*

$$\sum_{\forall \delta|p-1} \psi(\delta) = p-1.$$

Теорема 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 $N = \text{НОК}[n_1, n_2, \ldots, n_g]$.

Утверждение 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. $ka \equiv kb \pmod{km}$.

Утверждение 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. $a \equiv b \pmod{m}$.

Утверждение 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.

Утверждение 16

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

Утверждение 17

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

Утверждение 18

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

Утверждение 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.

Утверждение 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.

1.5. Теоремы о числе решений степенных сравнений

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

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 14

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

Теорема 15

Если $\delta = (n, p-1)$, то вычеты n-й степени по простому модулю $p > 2$ совпадают с вычетами степени d по этому модулю.

Теорема 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 $n \mid \operatorname{ind} a$.

Теорема 14*

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

Теорема 16

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

Теорема 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 $\bar{1}$. Важным частным случаем степенных сравнений являются сравнения второй степени. Из доказанных выше теорем вытекают следующие следствия, относящиеся к случаю $n = 2$.

Следствие 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 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 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 18

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

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

ГЛАВА 2

Алгоритмический минимум

2.1. Вычисление наибольшего общего делителя и его линейного представления

Для нахождения наибольшего общего делителя двух целых чисел без разложения их на множители используется *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. В данном алгоритме используется следующее утверждение: если $a = bq + r$, где $b \neq 0$, и число d делит 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 $d = \text{НОД}(a, b)$. Отсюда следует, что

$$\text{НОД}(a, b) = \text{НОД}(b, \textbf{MOD}(a, b)).$$

Алгоритм Евклида описывается следующим образом:

ВХОД: a и $b \neq 0$.

1. [Инициализация] $(a_0, a_1) := (a, b)$.
2. [Основной цикл] Пока $a_1 \neq 0$, выполнять
   $(a_0, a_1) := [a_1, \textbf{MOD}(a_0, a_1)]$.
3. Вернуть $d := a_0$.

ВЫХОД: $d = \text{НОД}(a, b)$.

Расширенный алгоритм Евклида

Для чисел, взаимно простых с модулем, операция деления по модулю определена как операция умножения на число, являющееся обратным по отношению к делителю. Для нахождения обратного элемента используется *расширенный алгоритм Евклида*, который позволяет вычислить линейное представление наибольшего общего делителя чисел a и b через значения этих чисел: $\text{НОД}(a, b) = ax + by$, где коэффициент при a есть обратный элемент

$x = a^{-1} \bmod b$ и коэффициент при b есть обратный элемент $y = b^{-1} \bmod a$. Расширенный алгоритм Евклида может быть представлен в виде:

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 $d = \text{НОД}(a, b) = ax + by$.

2.2. 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 ($\mathbf{Z}/N$) классов вычетов по модулю $N = n_1 n_2 \ldots n_g$, где $\forall\, i, j \in \{1, 2, \ldots, g\}$ $\text{НОД}(n_i, n_j) = 1$, может быть представлено в виде набора остатков от деления этого значения на каждый из сомножителей n_i, т. е. имеется взаимно однозначное соответствие $R \leftrightarrow (r_1, r_2, \ldots, r_g)$, где $R \in \mathbf{Z}/N$, $r_1 \in \mathbf{Z}/n_1$, $r_2 \in \mathbf{Z}/n_2$, …, $r_g \in \mathbf{Z}/n_g$.

Китайская теорема об остатках гласит следующее.

Теорема

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 $c_1 N/n_1 \equiv 1 \bmod n_1$, $c_2 N/n_2 \equiv$ $\equiv 1 \bmod n_2$, …, $c_g N/n_g \equiv 1 \bmod n_g$. 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 $i \neq j$ $n_i \Big| \dfrac{N}{n_j}$ (например $n_1 \Big| \dfrac{N}{n_2}$, $n_3 \Big| \dfrac{N}{n_2}$, …, $n_g \Big| \dfrac{N}{n_2}$), 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 $\mathbf{Z}/N$, который ставится в соответствие набору значений $r_1, r_2, \ldots, r_g$. Подобрать необходимые значения $c_i N/n_i \equiv 1 \bmod n_i$ достаточно просто. Их можно вычислить по формуле $c_i = N/n_i\,[(n_i/N) \bmod n_i\,]$. Если дано некоторое $R \in \mathbf{Z}/N$, 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.

2.3. Алгоритм быстрого возведения в степень по модулю

Пусть требуется вычислить значение $S = a^W \bmod n$. Представим степень W в виде разложения по степеням числа 2:

$$W = w_{g-1} 2^{g-1} + w_{g-2} 2^{g-2} + \ldots + w_2 2^2 + w_1 2^1 + w_0,$$

где w_i есть цифра 0 или 1.

Преобразуем $S = a^W \bmod n$ следующим образом:

$$\begin{aligned} S = a^W \bmod n &= a^{w_{g-1}2^{g-1} + w_{g-2}2^{g-2} + \ldots + w_2 2^2 + w_1 2^1 + w_0} \bmod n = \\ &= (a^2)^{w_{g-1}2^{g-2} + w_{g-2}2^{g-3} + \ldots + w_2 2^1 + w_1 2^0} \cdot a^{w_0} \bmod n = \\ &= ((a^2)^2)^{w_{g-1}2^{g-3} + w_{g-2}2^{g-4} + \ldots + w_2 2^0} \cdot (a^2)^{w_1} \cdot a^{w_0} \bmod n = \\ &= (\ldots((a^2)^2 \ldots)^2)^{w_{g-1}} \cdot \ldots \cdot (a^8)^{w_3} \cdot (a^4)^{w_2} \cdot (a^2)^{w_1} \cdot a^{w_0} \bmod n. \end{aligned}$$

Из последней формулы нетрудно вывести следующий псевдокод, описывающий алгоритм быстрого возведения в степень:

ВХОД:

1. $S := 1$ и $c := a$ {Присвоить начальные значения переменным S и c}
2. For $i := 0$ to $g - 1$ do {Основной цикл}

   2.1. If $w_i = 1$, then $S := Sc \bmod n$. Otherwise go to step 2.2.

   2.2. $c := c^2 \bmod n$.

ВЫХОД: $S = a^W \bmod n$.

В более понятном и удобном для программирования виде алгоритм быстрого возведения в степень записывается следующим образом.

ВХОД: Целочисленные значения n, $a > 0$ и $W \geq 0$.

1. Инициализируем переменные $S := 1$, $V := W$ и $c := a$.
2. Если $V = 0$, то СТОП.
3. Если $V \bmod 2 = 1$ (т. е. текущее значение V является нечетным), то присваиваем новые значения переменным $S := Sc \bmod n$ и $V := (V - 1)/2$ и переходим к шагу 5. В противном случае переходим к шагу 4.
4. Выполняем операцию присваивания $V := V/2$.
5. Выполняем операцию присваивания $c := c^2 \bmod n$.
6. Переходим к шагу 2.

ВЫХОД: Значение $S = a^W \bmod n$.

Нетрудно подсчитать, что средняя сложность данного алгоритма составляет $1.5g$ операций умножения двух g-битовых чисел плюс $1.5g$ операций деления $2g$-битовых чисел на g-битовое число. Для 1000-битовых и более длинных чисел данный алгоритм выполняется на ЭВМ достаточно быстро.

Если модуль может быть разложен на сравнительно небольшие простые делители, т. е. $n = p_1 p_2 \ldots p_g$, то возведение в степень по такому модулю может быть сильно упрощено, если использовать китайскую теорему об остатках. Сначала вычисляются вычеты $a^W \bmod p_i$ по каждому из простых делителей p_i, $i = 1, 2, \ldots, g$. Используя теорему Ферма, эти вычисления можно сделать достаточно быстрыми.

В результате получим следующую систему сравнений:

$$\begin{cases} a^W \equiv r_1 \bmod p_1, & 0 \le r_1 < p_1, \\ a^W \equiv r_2 \bmod p_2, & 0 \le r_1 < p_2, \\ \qquad\qquad \cdots\cdots \\ a^W \equiv r_g \bmod p_g, & 0 \le r_1 < p_g. \end{cases}$$

Полагая $x = a^W$ и решая по китайской теореме об остатках систему сравнений, приведенную выше, найдем значение $R \in \mathbf{Z}/n$, удовлетворяющее системе. Поскольку a^W также удовлетворяет рассматриваемой системе сравнений и все ее решения сравнимы между собой по модулю n, то $R \equiv a^W \bmod n$, т. е. $S = R$.

2.4. Нахождение первообразных корней

Показателями могут быть только делители функции Эйлера от модуля m, т. е. делители обобщенной функции Эйлера $L(m)$, которая является наибольшим возможным показателем по модулю m. Для модулей вида p^s и $2p^s$, где $s \ge 1$, имеем $L(m) = \varphi(m)$ и существуют первообразные корни. Если модуль является простым числом p, то количество чисел, относящихся к показателю γ, равно функции Эйлера от числа γ, т. е. $\psi(\gamma) = \varphi(\gamma)$. Чем меньше показатель, тем меньше существует чисел, относящихся к нему. Наибольшее число чисел относится к показателю $p-1$, т. е. имеется достаточно большое число первообразных корней и при случайном выборе чисел мы с большой вероятностью попадаем на них. Нахождение первообразного корня осуществляется путем случайного выбора числа α и проверкой выполнимости условия $\alpha^{\frac{p-1}{d_i}} \ne 1 \bmod p$ для всех простых делителей d_i числа $p-1$. Этот способ основан на следующем утверждении:

Пусть имеем разложение $p-1 = d_1^{s_1} d_2^{s_2} \ldots d_h^{s_h}$. *Если для каждого простого делителя* d_i *числа* $p-1$ *выполняется условие* $\alpha^{\frac{p-1}{d_i}} \ne 1 \bmod p$, *то число* α *является первообразным корнем* (*примитивным элементом*) *по модулю* p.

Доказательство

Допустим, что α не является первообразным корнем и относится к показателю $\delta < p-1$. Поскольку $\delta \mid p-1$, то $k = (p-1)/\delta$ есть простой или состав-

ной делитель числа $p-1$, т. е., по крайней мере, для одного из делителей d_i имеем $d_i \mid k$. Следовательно, число $\dfrac{p-1}{d_i\delta}$ является целым. По предположению имеем: $\alpha^{\delta} = 1 \bmod p \Rightarrow (\alpha^{\delta})^{\frac{p-1}{d_i\delta}} = 1 \bmod p \Rightarrow \alpha^{\frac{p-1}{d_i}} = 1 \bmod p$, что противоречит исходному условию.

2.5. Нахождение чисел, относящихся к заданному показателю

Случай простого показателя

Если длина простого делителя γ существенно меньше длины простого модуля, то нахождение чисел, относящихся к γ как к показателю, путем случайного выбора чисел a и проверки соотношения $a^{\gamma} = 1 \bmod p$ является вычислительно неэффективным (на самом деле практически невыполнимым). Для нахождения числа α, относящегося к простому показателю γ, используется следующий вычислительно эффективный способ.

1. Выбирается число b, превосходящее 1 и меньшее числа p.
2. Вычисляется значение $\gamma' = (p-1)/\gamma$ и число $z = b^{\gamma'} \bmod p$.
3. Если $z \neq 1$, то в качестве числа α взять число z. В противном случае повторить шаги 1–3.

Действительно, для полученного числа $z \neq 1$ имеем $z = b^{(p-1)/\gamma} \bmod p$. Следовательно, согласно теореме Ферма, имеем $z^{\gamma} \equiv b^{p-1} \equiv 1 \bmod p$, т. е. число z относится к показателю γ. Известно, что при выполнении условия $z^{\gamma} \equiv 1 \bmod p$ показатель числа z делит γ. Так как γ есть простое число, то оно и является показателем.

Случай составного показателя

Если требуется найти число α, относящееся к составному показателю γ, каноническое разложение которого имеет вид $\gamma = q_1^{\omega_1} q_2^{\omega_2} \ldots q_z^{\omega_z}$, то можно воспользоваться следующим алгоритмом:

1. Выбирается случайное число b, превосходящее 1 и меньшее числа p.
2. Вычисляется значение $\gamma' = (p-1)/\gamma$ и число $z = b^{\gamma'} \bmod p$.

3. Если $z = 1$, то перейти к шагу 1.
4. Если для каждого простого делителя q_i числа γ выполняется условие $z^{\frac{\gamma}{q_i}} \neq 1 \bmod p$, то в качестве числа α взять число z. В противном случае повторить шаги 1–4.

Докажем, что этот алгоритм действительно находит число, относящееся к показателю γ. Для полученного числа $\alpha \neq 1$ имеем $\alpha = b^{(p-1)/\gamma} \bmod p$. Согласно теореме Ферма, имеем $\alpha^{\gamma} \equiv b^{p-1} \equiv 1 \bmod p$. Допустим, что α относится к показателю $\delta < \gamma$. Тогда $\delta \mid \gamma$ и $k = \gamma/\delta$ есть простой или составной делитель числа γ, т. е., по крайней мере, для одного из делителей q_i имеем $q_i \mid k$. Следовательно, число $\frac{\gamma}{q_i \delta}$ является целым. По предположению имеем: $\alpha^{\delta} = 1 \bmod p \Rightarrow (\alpha^{\delta})^{\frac{\gamma}{q_i \delta}} \equiv 1 \bmod p \Rightarrow \alpha^{\frac{\gamma}{q_i}} \equiv 1 \bmod p$, что противоречит условию, проверяемому на шаге 4 алгоритма поиска числа α.

2.6. 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 $41\,041 = 7 \cdot 11 \cdot 13 \cdot 41$).
- *Тест Соловея–Штрассена* заключается в проверке равенств $\left(\frac{b}{p}\right) = 1$, где $\left(\frac{b}{p}\right)$ — символ Лежандра 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.)

2.7. Детерминистическая генерация больших простых чисел

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:

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

Затем выбирается некоторое число b и проверяется, выполняются ли для данного p_1 следующие два условия:

1. $b^{p_1 - 1} = 1 \pmod{p}$ и
2. $b^{\frac{p_1 - 1}{m_i}} \neq 1 \bmod p$ для всех $m_i \in \{m_1, m_2, \ldots, m_h\}$.

Если после нескольких попыток найдется некоторое b, которое удовлетворяет указанным выше двум соотношениям, то p является простым числом. Если такое число не найдено, то выбирается другой случайный набор простых чисел $m_1, m_2, \ldots, m_h$ из набора $q_1, q_2, \ldots, q_k$. Сформированное таким образом число p_1 имеет длину примерно в h раз больше средней длины чисел $q_1, q_2, \ldots, q_k$ (например, от $8h$ до $10h$ десятичных знаков). Можно аналогичным образом сформировать следующий набор простых чисел $\{p_1, p_2, \ldots, p_k\}$ и, используя их в качестве исходных, повторить рассматриваемую процедуру, формируя еще более длинные простые числа. Достоинством данного способа является то, что мы заведомо знаем разложение $p - 1$; кроме того, мы можем формировать это разложение таким образом, чтобы в нем содержались простые числа требуемой длины. Основным недостатком такого способа является то, что формируется только некоторый подкласс простых чисел заданной большой длины. Однако мощность этого подкласса может быть задана такой, что этим обстоятельством атакующий не сможет воспользоваться для раскрытия той или иной двухключевой криптосистемы, в которой будет использоваться данная процедура детерминистической генерации простых чисел.

Данный детерминистический тест основан на следующей ***теореме***.

Пусть p — целое нечетное число, превышающее 1. Если существует $b \le p-1$, такое что выполняются следующие условия: 1) $b^{p-1} = 1 \bmod p$ и 2) $b^{\frac{p-1}{m_i}} \neq 1 \bmod p$ для каждого простого делителя m_i числа $p-1$, то число p является простым.

Доказательство

Допустим, что p не является простым. Тогда функция Эйлера от p имеет значение меньшее чем $p-1$, т. е. $\varphi(p) < p-1$. Рассмотрим два случая: а) НОД$(b, p) = 1$ и б) НОД$(b, p) \neq 1$. В случае а) порядок числа b должен делить $\varphi(p) < p-1$, но по условию теоремы порядок b равен $p-1$. В случае б) не существует целых степеней n, для которых выполняется условие $b^n = 1 \bmod p$. В обоих случаях приходим к противоречию, которое доказывает утверждение теоремы. (Пояснение к случаю б): если НОД$(b, p) = \delta \neq 1$, то $\delta | b^n \bmod p$ для любого n, поскольку для остатка r от деления b^n на p имеем НОД$(b^n, r) = \delta$).

Способ по стандарту ГОСТ Р 34.10–94

Для генерации больших простых чисел в ГОСТ Р 34.10–94 используется детерминистический тест, основанный на следующей ***теореме***.

Пусть $p = qN + 1$, где q — нечетное простое число, N — четное число и $p < (2q+1)^2$. Число p является простым, если выполняются следующие два условия:

1) $2^{qN} = 1 \bmod p$ и

2) $2^N \neq 1 \bmod p$.

Доказательство

Пусть γ есть порядок числа 2 по модулю p и p имеет следующее каноническое разложение: $p = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_h^{\alpha_h}$. Ввиду условия 1) γ делит $p-1$, т. е. $\gamma | p-1$. В силу условия 2) γ не является делителем числа $\frac{p-1}{q}$. Отсюда следует, что $q | \gamma$. Согласно теореме Эйлера $2^{\varphi(p)} = 1 \bmod p$, следовательно, $\gamma | \varphi(p) \Rightarrow q | \varphi(p)$, где $\varphi(p) = p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1} \ldots p_h^{\alpha_h - 1} (p_1 - 1)(p_2 - 1) \ldots (p_h - 1)$. Пусть q совпадает с простым множителем p_i. Из такого допущения следует, что $p = qn'$ для некоторого натурального числа n. Однако по условию теоремы

имеем $p = qN + 1$. Поскольку $q > 1$ не может делить число 1, то приходим к противоречию, из которого следует, что q должно делить число $p_i - 1$, по крайней мере, для некоторого одного из значений $i \in \{1, 2, \ldots, h\}$.

Таким образом, существует некоторое натуральное $n \geq 2$, такое что имеем $p_i - 1 = qn$ и $p_i = qn + 1$. Следовательно, при некотором натуральном m получим:

$$p = mp_i = m(qn + 1) = qN + 1 \;\Rightarrow\; m = q(N - mn) + 1.$$

При некотором натуральном $s \geq 0$ имеем $m = qs + 1$ и

$$p = (qn + 1)(qs + 1).$$

Пусть p есть составное число, тогда $s \geq 2$ (поскольку N и n — четные числа, а $s = N - mn$), из чего следует $p \geq (2q + 1)^2$. Это противоречит условию теоремы, следовательно, $s = 0$ и число p является простым.

Схема построения алгоритма описывается следующим образом. Пусть требуется сформировать простое число p длины $t \geq 17$ бит. С этой целью строится убывающий набор натуральных чисел $t_0, t_1, \ldots, t_s$, где $t_0 = t$ и $t_s < 17$ бит, для которых выполняется условие $t_i = [t_{i-1}/2]$. Последовательно вырабатываются простые числа $p_s, p_{s-1}, \ldots, p_0$, причем длина числа p_i равна значению t_i для всех $i = 1, \ldots, s$. Исходное простое значение p_s формируется путем случайного выбора числа размером менее 17 бит и проверки на простоту методом пробного деления.

Генерация простого числа p_{i-1} по простому числу p_i осуществляется с использованием формулы

$$p_{i-1} = p_i N + 1,$$

где N — случайное четное число, такое что длина числа $p_i N + 1$ равна значению t_i. Число p_{i-1} считается полученным, если одновременно выполнены следующие два условия:

1) $2^{p_i N} = 1 \bmod p_{i-1}$;

2) $2^{N} \neq 1 \bmod p_{i-1}$.

Если хотя бы одно из условий не выполнено, то значение N увеличивается на 2, вычисляется новое значение p_{i-1}, которое снова проверяется на простоту по указанным двум условиям. Такая процедура выполняется до тех пор, пока не будет получено простое число p_{i-1}.

2.8. Извлечение квадратных корней по модулю

Извлечение квадратного корня по модулю используется как базовый примитив в ряде криптосистем. При составном модуле эта операция выполняется следующим путем: 1) разложение модуля n на простые множители: $n = p_1^{\omega_1} p_2^{\omega_2} ... p_z^{\omega_Z}$, 2) извлечение корня из заданного числа по каждому из простых модулей $p_1, p_2, \ldots, p_z$, и 3) последующее восстановление корня по составному модулю с помощью китайской теоремы об остатках. Вычисление корней по простому модулю сводится к одной или нескольким операциям возведения в степень по модулю. Сложность процедуры извлечения корня зависит от конкретного значения простого модуля. Наиболее простым является случай, когда модуль сравним с числом 3 по модулю 4: $p \equiv 3 \bmod 4$. Следующими по возрастанию сложности являются случаи $p \equiv 5 \bmod 8$ и $p \equiv 1 \bmod 8$ (случаи $p \equiv 3 \bmod 8$ и $p \equiv 7 \bmod 8$ относятся к случаю $p \equiv 3 \bmod 4$). При $p \equiv 1 \bmod 8$ используется общий алгоритм вычисления корней, который реализует операцию извлечения квадратного корня по произвольному простому модулю. Рассмотрим процедуру извлечения корней для указанных трех случаев.

Случай p ≡ 3 mod 4

Пусть a является квадратичным вычетом и требуется найти число x, такое что $x^2 \equiv a \bmod p$, где простое p удовлетворяет условию $p \equiv 3 \bmod 4$. Для квадратичных вычетов имеет место сравнение $a^{\frac{p-1}{2}} \equiv 1 \bmod p$. Умножая обе части этого сравнения на a, получаем: $a^{\frac{p+1}{2}} \equiv a \bmod p$. Поскольку $p \equiv 3 \bmod 4$, степень $\frac{p+1}{4}$ есть целое число, поэтому мы можем определить: $x = a^{\frac{p+1}{4}} \bmod p$. Возведением значения x в квадрат легко показать, что оно есть квадратный корень из числа a по модулю p. Таким образом, для рассматриваемого случая извлечение корня второй степени сводится к операции возведения в степень $\frac{p+1}{4}$ по модулю p:

$$\sqrt{a} \equiv a^{\frac{p+1}{4}} \bmod p.$$

Случай $p \equiv 5 \bmod 8$

Пусть a является квадратичным вычетом и требуется найти число x, такое что $x^2 \equiv a \bmod p$, где простое p удовлетворяет условию $p \equiv 5 \bmod 8$ (рис.1). Для квадратичных вычетов имеет место сравнение $a^{\frac{p-1}{2}} \equiv 1 \bmod p$. Поскольку $p \equiv 5 \bmod 8$, то при некотором натуральном k имеем: $p-1 = (8k+5)-1 = 4(2k+1)$. Поэтому $a^{\frac{p-1}{2}} = a^{2(2k+1)} \equiv 1 \bmod p$. Из последнего сравнения следует, что либо $a^{\frac{p-1}{4}} = a^{2k+1} \equiv 1 \bmod p$ (1), либо $a^{\frac{p-1}{4}} = a^{2k+1} \equiv -1 \bmod p$ (2). Если имеет место первый случай, то, умножая обе части сравнения (1) на a, имеем: $a^{\frac{p+3}{4}} = a^{2\frac{p+3}{8}} = (a^{\frac{p+3}{8}})^2 \equiv a \bmod p$, где $\frac{p+3}{8}$ есть целое число, откуда следует формула для вычисления квадратного корня

$$\sqrt{a} \equiv a^{\frac{p+3}{8}} \bmod p.$$

Если имеет место второй случай, то, умножая обе части сравнения (2) на -1, имеем: $a^{\frac{p-1}{4}} \cdot (-1) \equiv 1 \bmod p$. Теперь представим $-1 \bmod p$ как $b^{4k+2} \bmod p$, где b есть произвольный квадратичный невычет по модулю p. (Действительно, для невычета b имеем: $b^{\frac{p-1}{2}} = b^{\frac{8k+4}{2}} = b^{4k+2} \equiv -1 \bmod p$.) Таким образом, мы получили $a^{\frac{p-1}{4}} b^{4k+2} \equiv 1 \bmod p$ (3), где $\frac{p-1}{4} = 2k+1$ есть нечетное число. Умножая обе части сравнения (3) на a, получаем $a^{\frac{p+3}{4}} b^{4k+2} = a^{\frac{p+3}{4}} b^{\frac{p-1}{2}} \equiv a \bmod p$, где показатели степеней чисел a и b являются четными, поэтому мы можем определить $x = a^{\frac{p+3}{8}} b^{\frac{p-1}{4}} \bmod p$ (где показатели степеней чисел a и b являются натуральными числами).

Возведением значения x в квадрат легко показать, что оно есть квадратный корень из числа a по модулю p: $x^2 = a^{\frac{p+3}{4}} b^{\frac{p-1}{2}} \equiv a \bmod p$.

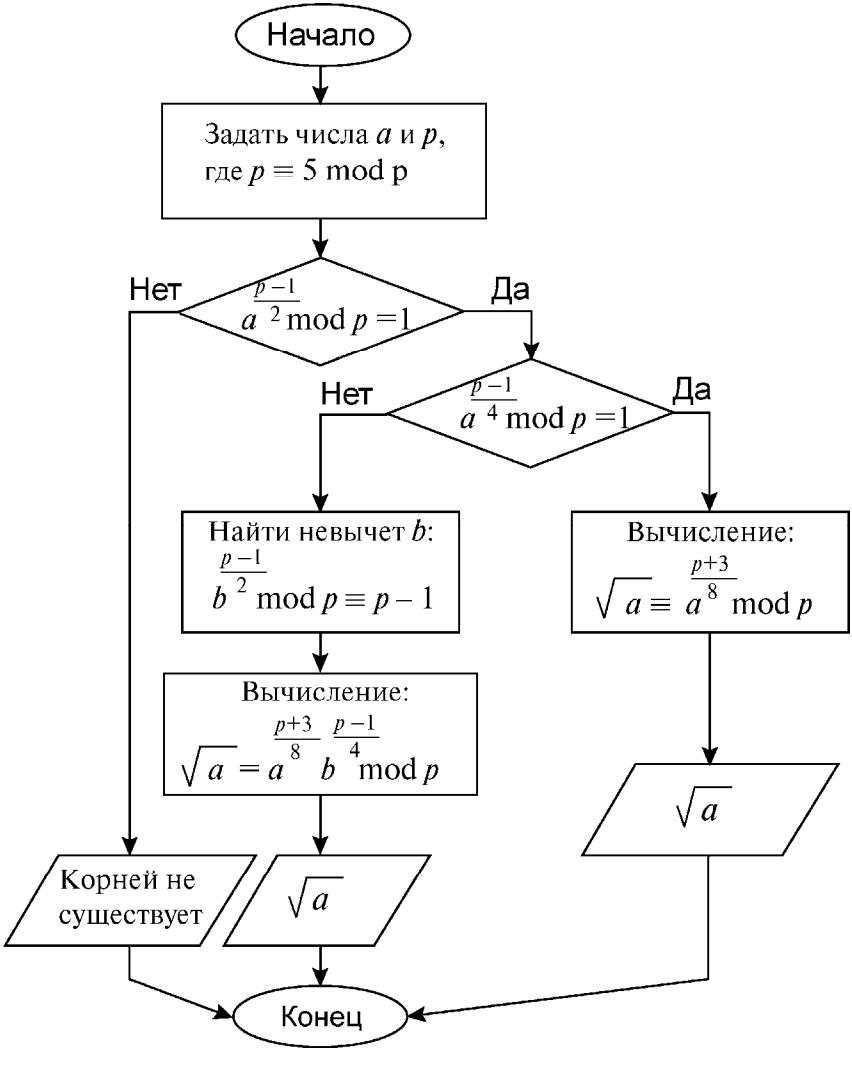

Рис. 1. Схема алгоритма вычисления квадратного корня по простому модулю p (случай $p \equiv 5 \bmod 8$)

Таким образом, для случая $a^{\frac{p-1}{4}} \equiv -1 \bmod p$ для вычисления квадратного корня может быть использована следующая формула:

$$\sqrt{a} = a^{\frac{p+3}{8}} b^{\frac{p-1}{4}} \bmod p .$$

При использовании этой формулы предварительно следует найти квадратичный невычет b, что осуществляется случайным выбором числа $b \le p-1$, за которым следует проверка выполнимости условия $b^{\frac{p-1}{2}} \bmod p = p-1$. Поскольку вероятность того, что случайное число является невычетом, равна 50 %, то нахождение квадратичного невычета требует в среднем выполнения двух попыток.

Случай произвольного простого модуля

Пусть a является квадратичным вычетом и требуется найти число x, такое что $x^2 \equiv a \bmod p$, где p — произвольное простое число. В этом общем случае задача решается с использованием определенного расширения приемов, примененных в случае $p \equiv 5 \bmod 8$. Для произвольного p можно записать:

$$p-1 = 2^t r,$$

где $t \ge 1$ и r — нечетное число. Пусть для вычета a и любого невычета b справедливо сравнение

$$a^S b^Z \equiv 1 \bmod p, \qquad (4)$$

где S — нечетное число, а Z — четное число или ноль. Тогда, умножая обе части последнего сравнения на a, получаем $a^{S+1} b^Z \equiv a \bmod p$, следовательно, можно определить значение $x = a^{(S+1)/2} b^{Z/2} \bmod p$, которое является квадратным корнем из a (это доказывается простым возведением значения x в квадрат). Для того чтобы найти представление единицы в виде (4), воспользуемся сравнением $a^{\frac{p-1}{2}} \equiv 1 \bmod p$, представив его в виде $a^{\frac{p-1}{2}} b^Z \equiv 1 \bmod p$, т. е. в виде, аналогичном (4), где в общем случае $S = (p-1)/2$ является четным и $Z = 0$. Рассмотрим сравнение (4) с начальными значениями $S = (p-1)/2$ и $Z = 0$, в котором осуществим ряд последовательных шагов одновременного деления обоих показателей степеней чисел a и b на два (на одном шаге выполняем две операции присваивания $S \leftarrow S/2$ и $Z \leftarrow Z/2$), пока не получим нечетное S. При этом перед некоторыми шагами деления к значению Z будем прибавлять число $(p-1)/2$, что соответствует умножению левой части (4) на $b^{\frac{p-1}{2}} \equiv -1 \bmod p$. Выполнение операции $Z \leftarrow Z + (p-1)/2$ будем осуществлять, если перед выполнением шага деления или при достижении условия прекращения цикла деления имеет место $a^S b^Z \equiv -1 \bmod p$. Заметим, что если