Эссе по курсу: Защита информации
на тему: Алгоритм быстрого возведения в степень
Московский физико-технический институт

25 декабря 2023 г.

Студент:	Михалун Д.О.
Преподаватель:	Семака В.Ю.
Группа:	Б01-003

Содержание

1 Введение

В современном мире, где большинство операций и передача данных осуществляются с использованием компьютерных технологий, безопасность информации становится одной из самых важных проблем. Основной математической операцией, применяемой в защите информации, особенно в криптографии, является возведение числа в степень.

Примеры использования возведения в степень в защите информации:

1. Шифрование: Возведение в степень используется при выполнении операций шифрования и дешифрования. Например, алгоритм шифрования RSA использует возведение в степень для шифрования сообщения с помощью публичного ключа и дешифрования с помощью соответствующего приватного ключа.

2. Проверка подлинности: Возведение в степень может использоваться для проверки подлинности данных при помощи электронной подписи

3. Реализация математических алгоритмов: возведение в степень позволяет реализовать различные математические алгоритмы, которые применяются в криптографии. Например: генерация простых чисел использует возведение в степень по модулю.

В данном эссе речь пойдет об основных алгоритмах возведения в степень, а именно - возведения в степень по модулю, так как криптография оперирует с модульной арифметикой. Описана сложность этих методов и показано, почему возведение числа в степень по простому модулю является важной частью шифрования. Кроме того, будут описаны основные математические алгоритмы, в которых применяется возведение в степень по модулю.

2 Метод повторяющихся возведения в квадрат и умножения

Пусть требуется вычислить: y = $a^x \mod p$

Введем переменную $t = [log2(x)]$

Вычисляем числа ряда

a, $a^2, a^4, \ldots a^{2t}$ mod p (1.1) Каждое число вычисляется путем умножения предыдущего числа на самого себя по модулю p

Переведем x в двоичную систему: (x$_t$, x_{t-1}, $\ldots$, $x_0)_2$ Тогда число y = $a^x modp$ может быть получено так: $y = \prod_{i=0,\ldots,t}$a$^{(x_i*2^i)}$(1.2)

Приведем наглядный пример использования этого алгоритма.

Допустим мы хотим вычислить 5^{100} по модулю 7

1. Вычислим (a, $a^2, a^4, \ldots a^64$): a = 5 a^2 = 5*5 = 25 = 4 (mod 7) a^4 = 4*4 = 16 = 2 (mod 7) a^8 = 2*2 = 4 (mod 7) Аналогично вычислим a^{16} , a^{32}, a^{64} получим упорядоченный набор (5, 4, 2, 4, 2, 4, 2)

2. Запишем показатель степени в двоичной системе исчисления: 100 = 1100100_2

3. Воспользуемся формулой (1.2): 2*4*1*1*2*1*1 = 8 = 1 (mod 7)

Алгоритмы реализуются двумя способами: слева-направо и справа-налево, в зависимости от того, в каком порядке просматриваются биты показателя степени (от младшего к старшему или от старшего к младшему)

Лемма 2.1. (о сложности вычислений). Количество операций умножения n при вычислении $y = a^x$ mod p не превосходит $\log x$

Доказательство:
Вычисление ряда (1.1) требует t умножений, ряда (1.2) - не более, чем t.
$n <= t = [log2x] <= log2x$

Область применения:

Данный метод применяется в случае, когда степень x - простое число или раскладывается на произведение двух простых чисел.
В противном случае применяется метод с использованием Китайской теоремы об остатках, который будет рассмотрен далее.

3 Метод с использованием Китайской теоремы об остатках

Для описания данного метода потребуется теорема:

Теорема 3.1. Китайская теорема об остатках

Пусть натуральные числа $m_1, m_2, \ldots, m_n$ попарно взаимно просты.
Тогда для любых $a_1, \ldots, a_n$ э Z :0 <= a$_i$ $< m_i$, существует N э N :N = r$_i(moda_i)$; и существует N_1, N_2 э N :N$_1$ тождественно равно N_2 (mod $a_1 * a_2 ... * a_n$)

Описание метода:

Пусть нам требуется вычислить $y = a^x$ mod p.

Пусть p разбивается на n простых множителей p_1, ..., p_n.

Сначала вычисляются вычеты a^x mod pi при помощи теоремы Ферма.

В результате получаем систему сравнений: $a^x = r_1 modp_1, 0 <= r_1 < p_1 a^x = r_2 modp_2, 0 <= r_2 < p_2 \ldots \ldots . a^x = r_n modp_n, 0 <= r_n < p_n$

Положим $a^x = t$.

Решая по Китайской теореме об остатках эту систему сравнений относительно t, находим значение R э Z/n.

Поскольку a^x - тоже решение этой системы, и все решения сравнимы между собой, то a^x = R.

Область применения:

В криптографии в большинстве случаев возведение в степень осуществляется по простому модулю, поэтому данный метод применяется редко.

4 Одностороняя функция

Обратная функция к возведению в степень по модулю - дискретное логарифмирование. Данная операция вычисляется гораздо дольше, чем возведение в степень. Наиболее лучшие алгоритмы вычисления данной функции:

Алгоритмы с экспоненциальной сложностью

1. Алгоритм Шенкса (алгоритм больших и малых шагов, baby-step giant-step)
2. Алгоритм Полига — Хеллмана
3. p-Метод Полларда

Данные алгоритмы имеют экспоненциальную сложность - O($p^{1/2}$), где p - модуль, по которому вычисляется степень.
Именно высокая вычислительная сложность этих алгоритмов определяет стойкость криптографических схем. Функции, подобные функции возведения в степень по модулю, имеют собственное определение - односторонние функции.

Односторонняя функция в криптографии - это функция, которая вычисляется достаточно просто в прямом направлении, но вычисление обратной функции - очень сложная задача.

Покажем, что при больших p функция возведения в степень по модулю p действительно односторонняя.

Выше мы оценили время вычисления прямой функции как не большее чем $log2p$

Допустим для вычисления обратной функции мы будем использовать метод "шаг младенца шаг великана"(baby-step giant-step) (t $\sim 2\sqrt{p}$)

Количество десятичных знаков в записи p	Вычисление (2.3) ($2 \log p$ умножений)	Вычисление (2.4) ($2 \cdot \sqrt{p}$ умножений)
12	$2 \cdot 40 = 80$	$2 \cdot 10^6$
60	$2 \cdot 200 = 400$	$2 \cdot 10^{30}$
90	$2 \cdot 300 = 600$	$2 \cdot 10^{45}$

Рис. 1: *Таблица: количество умножений для вычисления прямой и обратной функции*

Можно сделать вывод, что с увеличением числа знаков в десятичной записи p сложность возведения в степень по этому модулю растет линейно, в то время как сложность вычисления обратной функции растет экспоненциально.

5 Метод возведения в степень в математических алгоритмах

Извлечение корней

Одна из операций, где применяется возведение в степень по модулю - извлечение корней. Извлечение квадратного корня по модулю - важная операция для криптографии. Алгоритм извлечения корня зависит от самого значения модуля. Наиболее простой случай: p = 3 mod 4. Корнем уравнения x^2 = a mod p является число $x = a^{((p+1)/4)} mod p$.

Если модуль составной, то операция сводится к нахождению корня числа по каждому из простых модулей. Затем корень восстанавливается при помощи Китайской теоремы об остатках.

Генерация простых чисел

Возведение в степень по модулю применяется также для генерации простых чисел. Алгоритм генерации простых чисел заключается в следующем:

1. Генерируется случайное число
2. Сгенерированное число проверяется на простоту с помощью тестов Число, прошедшее большое количество тестов называется псевдопростым.

Основные применяемые тесты: тест Ферма и тест Соловея-Штрассена. Оба теста сводятся к операции возведения в степень по модулю.
Тест Ферма: $a^{(p-1)} = 1$ mod p
Тест Соловея-Штрассена: $a^{(p-1)/2} = (a/p)$ mod p

Отметим, что данные тесты не гарантируют простоту числа. Они лишь указывают на то, что число является простым с большой вероятностью.

Факторизация составных чисел

Крайне важная математическая операция в криптографии - факторизация составных чисел. Как было рассмотрено выше, факторизация чисел применяется в методах, опирающихся на Китайскую теорему об остатках. Данная операция также реализуется с помощью возведения в степень. Рассмотрим один из методов реализации: ро-метод Полланда.
Выбирается простой многочлен в Z/Zp, например: $f(x) = x^2 + 1$, и отправная точка x0.
Вычисляется последовательность $x_{i+1} = f(xi), i = 0{,}1\dots$
Среди элементов последовательности выбираются такие x_i, x_j: $x_i! = x_j modp$, но $x_i = x_j modp_i$, где p_i - некоторый делитель числа p.
Тогда искомый делитель вычисляется так: $p_k =$НОД$(x_i - x_j, p)$
Рассмотрим пример: разложим 91 на простые множители. возьмем f(x) = $x^2 + 1$,$x_0 = 1$. Получаем: $x_1 = 2, x_2 = 5, x_3 = 26, x_4 = 40$,....НОД$(x_3 - x_2, 91) = 7$. Итак, мы нашли делитель числа 91 - 7.

Эллиптические кривые

Теория эллиптических кривых активно используется в криптографии. Основная криптографическая операция на эллиптической кривой - вычисление композиции Q = [m]P = P + P + P . . . + P, где P - точка на кривой. Операция композиции выполняется следующим образом:
$k = (3x_1^2 + a)/2y_1$
$x_3 = k^2 - x_1 - x_1$
$y_3 = k(x_1 - x_3) - y_1$, где(x_1,y_1) - координаты точки $P(x_1,y_1)$, a - коэффициент уравнения эллиптической кривой: $Y^2 = X^3 + aX + b$

6 Заключение

В данной статье были рассмотрены различные методы возведения в степень по модулю, которые широко используются в современной математике и криптографии. Описано, как эти методы могут быть применены для решения различных задач, таких как: вычисление корней, факторизация чисел и генерация простых чисел. Эти методы являются наиболее эффективными и упрощают вычислительную сложность задач. В заключении можно отметить, что методы возведения в степень по модулю являются важным инструментом в современной математике и криптографии. В статье подробно были описаны следующие алгоритмы:

1. Вычисление квадратного корня числа по модулю. Был рассмотрен частный случай, когда p = 3 mod 4. Вычисление корней применяется для факторизации модуля RSA.

2. Генерация простых чисел. Операция возведения в степень по модулю применяется в тестах, определяющих простоту числа. Простые числа используются в системах шифрования, например в RSA - открытый и закрытый ключи формируются при помощи простых чисел.

3. Факторизация составных чисел. Однако, несмотря на наличие алгоритмов, данная операция является экспоненциально-сложной и на ее вычислительной сложности построена система шифрования RSA.

4. Вычисление точек на эллиптической кривой. На базе эллиптических кривых строятся современные криптографические алгоритмы. Для вычисления операции композиции точек на кривой используется метод возведения числа в степень.

Возведение в степень активно применяется в следующих областях криптографии:

1. Асимметричное шифрование. Самый известный представитель асимметричных шифров - шифр RSA. В алгоритме RSA шифрование и дешифрование выполняется при помощи возведения числа в степень по модулю.

2. Проверка подлинности автора. Проверка ЭЦП(электронной цифровой подписи) проводится также при помощи рассмотренных методов. Например, вычисление подписи в схемах на базе RSA и Эль-Гамаля проводится при помощи возведение в степень.

3. Криптосистемы с открытым ключом. Самая первая система с открытым ключом - система Диффи - Хеллмана. Ее реализация строится на возведении числа в степень. Другой шифр - шифр, предложенный Шамиром (Adi Shamir), был первым, позволяющим организовать обмен секретными сообщениями по незащищенному каналу. Его реализация также основывается на возведении числа в степень по модулю.

4. Криптосистемы на эллиптических кривых. Преимущество таких криптосистем заключается в том, что они менее трудоемкие, чем обычные, при равной стойкости, либо более стойкие при равной трудоемкости. Для вычисления точек эллиптической кривой используется возведение в степень.

В каждой из этих областей, метод быстрого возведения в степень позволяет эффективно реализовывать алгоритмы. Рассмотрены далеко не все задачи, которые можно решать с помощью методов возведения числа в степень по модулю. Их важность и разнообразие применения делают эти методы ключевыми инструментами в современной математике и криптографии. При этом, развитие и совершенствование этих методов продолжается, что открывает новые возможности для их применения в будущем.

7 Список использованной литературы

1. Рябко Б. Я., Фионов А. Н. Основы современной криптографии для специалистов в информационных технологиях — Научный мир, 2004. — 15 с., 16 с., 17 с., 18 с., 21с., 22с., 30с., 31с., 49-51 сс., 52 с., 53 с., 86 с., 87 с., 91 с., 94 с. — ISBN 978-5-89176-233-6

2. Молдовян Н. А. Теоретический минимум и алгоритмы цифровой подписи. — СПб.: БВХ-Петербург: Книжный Дом «ЛИБРОКОМ», 2010. — 15 с., 21 с., 22 с., 25 с., 55 с., — ISBN 978-5-9775-0585-7.

3. Коблиц Н. Курс теории чисел и криптографии — 2-е издание — М.: Научное издательство ТВП, 2001. — 155 с. — ISBN 978-5-85484-014-9, 978-5-85484-012-5