Санкт-Петербургский Государственный университет
Фундаментальная математика и механика
Теория функции

ДИПЛОМНАЯ РАБОТА

студента 14.C03-мм группы
Чамова Дмитрия Романовича

Явные законы взаимности и применения

Научний руководитель,
доктор физ - мат. наук, профессор,
Сергей Владимирович Востоков

Рецензент,
доцент кафедры алгоритмической математики
Санкт-Петеербургского электротехнического университета им. Ленина (ЛЭТИ),
кандидат физ - мат. наук,
доцент по кафедре математики,
Наталия Александровна Жарковская

Санкт-Петербург
-2019 г.-

Saint-Petersburg State University
Fundamental Mathematics and Mechanics
Function theory

Dmitrij Chamov

Graduation Thesis

Explicit reciprocity laws and application

Thesis supervisor,
Doctor of Physico-Mathematical Sciences,
Full Professor,
S. V. Vostokov

Thesis Reviewer,
Saint-Petersburg Electrotechnical University "LETI",
associate professor of the Department of Algorithmic mathematics,
PhD in Mathematics (Number Theory),
Associate Professor in Mathematics,
Natalia Alexandrovna Zharkovskaia

Saint-Petersburg
-2019-

Содержание

1 Введение

В дипломе рассматриваются элементы теории чисел и их использование в современных системах защиты информации. Теория чисел очень древняя наука, которая сейчас переросла в направление "Арифметическая геометрия". Но даже самые давние фундаментальные результаты этой науки только в наше время находят в востребованной ныне - криптографии(см. например [3]). Это можно увидеть на примере теоремы Эйлера из теории чисел, которая была доказана в середине XVIII века и нашла применение в созданной в 1978 году первом современном методе криптографии RSA(см. ниже).

Во второй части диплома будет рассказано, как окончательное решение 9-й проблемы Гильберта в 1978 году(см. [2]) дало в 2003 г. применение в криптографии.

2 Теория чисел

2.1 Функция Эйлера

Определим функцию Эйлера $\varphi(m)$ для целого $m > 1$ следующим образом.

Рассмотрим все остатки при делениии на число $m : 0, 1, 2, \ldots, m-1$ и сосчитаем количество взаимно-простых с m остатков. Это число и будем называть функцией Эйлера.

Рассмотрим два частных случая:

1. Если p — простое число, то ясно, что $\varphi(p) = p - 1$.

2. Если p и q — два различных простых числа, то $\varphi(pq) = (p-1)(q-1)$.

2.2 Теорема Эйлера

Теорема 1 (Эйлер)**.** *[1] Пусть a и m — взаимно простые числа, тогда выполнено сравнение*

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

3 Расширенный Алгоритм Евклида

Для понимания выполняемых операций в криптографических преобразованиях одним из наиболее часто используемых инструментов является расширенный алгоритм Евклида для нахождения мультипликативно обратного по модулю некоторого целого числа. Надо отметить, что в общем случае применение этого алгоритма значительно шире и затрагивает не только криптографические преобразования, но и, например, теорию алгебраического кодирования. Однако здесь мы остановимся только на возможностях этого замечательного алгоритма для наших целей, а именно, вычисления числа x обратного по умножению числу y по модулю целого числа p.

$$x : x \cdot y \equiv 1 \pmod{p}.$$

Необходимым условием нахождения такого x, очевидно, является взаимная простота y и p. В расширенном алгоритме Евклида используются вспомогательные элементы u_i связанные рекуррентной формулой $u_{i+1} = q_i \cdot u_i + u_{i-1}$, где $u_{-1} = 0, u_0 = 1$ и q_i - частное, полученное на i-ом шаге алгоритма. Приведем теперь последовательность шагов алгоритма:

(1) $p = y \cdot q_1 + r_1$, $u_1 = q_1 \cdot u_0 + u_{-1}$, где q_1, r_1 соответственно частное и остаток от деления p на y.

(2) $y = r_1 \cdot q_2 + r_2$, $u_2 = q_2 \cdot u_1 + u_0$,

(3) $r_1 = r_2 \cdot q_3 + r_3$, $u_3 = q_3 \cdot u_2 + u_1$,
$\ldots$

(i) $r_{i-2} = r_{i-1} \cdot q_i + r_i$, $u_i = q_i \cdot u_{i-1} + u_{i-2}$,
$\ldots$

(l) $r_{l-2} = r_{l-1} \cdot q_l + 1$, $u_l = q_l \cdot u_{l-1} + u_{l-2}$. Это последний шаг алгоритма, так как остаток, полученный на этом шаге равен 1 - наибольшему общему делителю чисел p и y.

Искомое значение x определяется следующим образом:

$$x \equiv (-1)^l \cdot u_l \pmod{p}.$$

4 Приложения в криптографии

4.1 Несимметричная криптография

Идея передачи секретной информации по незащищенному каналу была первоначально предложена James H. Ellis в 1970 году. Затем Ellis, Cocks и Williamson в 1973 году предложили идею алгоритма RSA, но результат был засекречен в Великобритании и лишь 18 декабря 1997 году Clifford Cocks анонсировал его для общественности. Рассмотрим этот алгоритм трёх британцев.

4.1.1 Алгоритм WCE

В качестве секретного ключа выбираются два больших простых числа p и q. Открытым ключом является их произведение $N = p \cdot q$. Сообщение m должно удовлетворять следующим ограничениям: это целое положительное число, $m < N$. Для того чтобы зашифровать сообщение его необходимо возвести в степень открытого ключа N и результат взять по модулю N (то есть вычислить остаток от деления).

$$e = m^N \pmod{N}$$

Таким образом, для шифрации достаточно знание только открытого ключа. При этом отметим здесь, что открытый ключ в алгоритме WCE представляет собой одно число N, являющееся произведением двух секретных простых чисел p и q таких что $(p, (q-1)) = 1$, $(q, (p-1)) = 1$, где (a, b) — наибольший общий делитель для любых целых a, b.

Для того чтобы расшифровать сообщение e необходимо знание секретного ключа. Первоначально находится фукнция Эйлера $\varphi(N) = (p-1)(q-1)$ и вычисляется вспомогательное число c

$$c = N \pmod{\varphi(N)}.$$

Затем вычисляется секретный ключ d

$$d \cdot c = 1 \pmod{\varphi(N)}.$$

Для этого используется расширенный алгоритм Евклида. Здесь следует заметить, что автоматически выполняется очень важное свойство для корректной работы расширенного алгоритма Евклида. А именно - наибольший общий делитель чисел N и $\varphi(N)$ равен 1. И, наконец, зашифрованное сообщение e возводится в степень d.

$$m = e^d = m^{c \cdot d} = m^{1 \pmod{\varphi(N)}} \equiv m \pmod{N}.$$

А теперь посмотрим официальную, наиболее часто встречающуюся версию появления несимметричной криптографии.

4.1.2 Алгоритм шифрования RSA

В 1978 году Рональд Райвест, Ади Шамир и Леонард Адлеман запатентовали и опубликовали свой алгоритм получивший в дальнейшем название RSA [6]. В этом же номере журнала известный математик и ученый Мартин Гарднер по согласию авторов алгоритма, опубликовал математическую задачу, получившую название RSA-129. В условии задачи он указал два числа n и e - открытый ключ и зашифрованный текст. Длина числа n составляла 129 десятичных знаков, а число $e = 1007$. За расшифровку текста предполагалась премия в 100 долларов. Шифр удалось взломать через 17 лет — около 600 человек объединились в сеть и усилиями 1600 компьютеров за полгода смогли прочитать фразу в 1995 году:

«The Magic Words are Squesmish Ossifrage»[1].

Основные этапы алгоритма RSA

- **Выбор секретного ключа и вычисление открытого ключа**

  1. Выбираем большие простые числа p и q с близким количеством цифр, после чего вычисляем $N = pq$.
  2. Вычисляем $\varphi(N) = (p-1)(q-1)$.
  3. Случайным образом выбираем число c, взаимно простое с $\varphi(N)$.
  4. С помощью расширенного алгоритма Евклида вычисляем число d, такое что $c \cdot d = 1 \pmod{\varphi(N)}$.

  Опредление 1. *Число d — секретный ключ, так же как и числа p и q.*

  Опредление 2. *Пара (c, N) — открытый ключ, который распространяется открыто.*

- **Шифрация сообщений с использованием открытого ключа**

  Сообщение — любое положительное целое число m не превосходящее N. При шифрации используется открытый ключ:

  $$e \equiv m^c \pmod{N}.$$

- **Дешифрация с использованием секретного ключа**

  Возводим число e в степень d и ищем остаток числа e^d при делении на N. Это будет искомое число m, так как

[1] «Волшебные слова — это брезгливая скопа».

$$e^d = m^{cd} \equiv m^{1+k\cdot\varphi(N)} \equiv m + l \cdot N \equiv m \pmod{N}.$$

Замечание 1. *Если число N имеет 100 цифр, то имеется не менее $4 \cdot 10^{42}$ простых числа, которые могут делить число N. Если компьютер выполняет 1 миллион операций в секунду, то ему понадобится примерно 10^{32} лет для вычисления $\varphi(N)$.*

Замечание 2. *В алгоритме RSA, использованном Гарднером для своего конкурса, использовались 64 и 65-значные простые числа.*

Замечание 3. *Сейчас для алгоритма RSA используют 150-значные простые числа.*

4.2 Электронная подпись

В предыдущем разделе мы посмотрели каким образом можно создать общий секретный ключ, используя для этого открытый прослушиваемый канал связи. Однако шифрация решает лишь одну из трех основных задач информационной безопасности - обеспечение конфиденциальности хранимой, обрабатываемой и передаваемой информации. К сожалению, это не позволяет предотвратить незаметное изменение критически важной информации [4]. Очевидно, что злоумышленник, зная открытый ключ, которым было зашифровано исходное сообщение, может легко заменить его на другое [5]. Для того, чтобы этого нельзя было сделать, требуется использовать некоторую секретную информацию - секретный ключ. Когда говорят про электронную подпись, то обязательно упоминается некоторая однонаправленная функция - хэш-фукнция, позволяющая сообщение любого размера преобразовать в "отпечаток"фиксированной длины(например 256 бит). Такое преобразование и выполняется с помощью хэш-функции. В английском языке одним из значений слова "hash"является "путаница". И действительно при выполнении хэш-преобразования исходная информация "запутывается"так, что распутать(восстановить) ее обратно практически не представляется возможным. Для реализации подписи исходная информация сначала хэшируется, а затем подписывается с помощью секретного ключа. Таким образом возникает первая уязвимость подписи - так называемая коллизия при вычислении хэш-функции. Очевидно, если два разных сообщения имеют один и тот же результат хэш-функции, то и подписи у этих сообщений будут одинаковые. Таким образом, можно просто подставить подпись одного сообщения под другим. Существуют два вида электронной подписи:

- отрицаемая подпись,
- неотрицаемая подпись.

Отрицаемая подпись подразумевает использование одного и того же секретного ключа и при вычислении и при проверке электронной подписи. В этом случае, очевидно, обе стороны могут подписать сообщение и невозможно будет доказать кто же из них на самом деле подписал документ. Неотрицаемая подпись использует при вычислении секретный ключ пользователя, а при проверке - его открытый ключ. Такой вариант позволяет говорить о том, что подпись может быть сформирована только одним лицом - обладателем секретного ключа, в то время как проверить подпись может любой, кому известен его открытый ключ. Как мы с вами уже видели на примере алгоритмов несимметричного шифрования, знание открытого ключа не дает возможности вычислить соответствующий ему секретный ключ.

4.3 Электронная подпись на билинейном преобразовании

Метод для создания электронной подписи, который сейчас будет предложен, использует упрощенный вид спаривания в явном законе взаимности, полученном С. В. Востоковым в работе [2].

Множество целых чисел, взаимно простых с p:

$$\mathbb{Z}^{(p)} = \{a \in \mathbb{Z} | \text{НОД}(a, p) = 1\}.$$

Из свойств взаимно-простых чисел ясно, что умножение оставляет числа из $\mathbb{Z}^{(p)}$ в этом же множестве.

Пусть $\mathbb{N}^+$ — множество натуральных чисел с операцией сложения. Зададим спаривание

$$\begin{gathered}\left\langle , \right\rangle_p \colon \mathbb{Z}^{(p)} \times \mathbb{N}^+ \to \mathbb{Z} \pmod p \\ \left\langle a, n \right\rangle_p = l(a) \cdot n \pmod p \\ l(a) = \frac{\log(a^{p-1})}{p}\end{gathered}$$

Здесь $\log(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \ldots$

Определение 3. *Число a называем числом Виферих а, если $a^{p-1} \equiv 1 \pmod{p^2}$. В противном случае будем называть антивиферихов ым.*

Утверждение 1. *Спаривание $\left\langle , \right\rangle_p$ является билинейным, то есть*

$$\begin{gathered}\left\langle ab, n \right\rangle_p = \left\langle a, n \right\rangle_p + \left\langle b, n \right\rangle_p \text{ для любых } a \text{ и } b \text{ из } \mathbb{Z}^{(p)}; \\ \left\langle a, n+m \right\rangle_p = \left\langle a, n \right\rangle_p + \left\langle a, m \right\rangle_p \text{ для любых } n \text{ и } m \text{ из } \mathbb{N}^+.\end{gathered}$$

Кроме того, это спаривание невырожденно для антивиферихова числа a, то есть для такого a найдется $n \in \mathbb{N}^+$ такое, что $\left\langle a, n \right\rangle_p = 1 \pmod p$.

Доказательство. 1. Билинейность по второму аргументу очевидна, а по первому следует из свойств логарифма.

2. Невырожденность. Пусть число a — антивиферихово. Тогда

$$\tfrac{a^{p-1}-1}{p} \text{ не делится на } p.$$

Поэтому

$$l(a) = \frac{\log(a^{p-1})}{p} = \frac{\log(1+\frac{a^{p-1}-1}{p}\cdot p)}{p} = \frac{\frac{a^{p-1}}{p}\cdot p}{p} - \frac{\left(\frac{a^{p-1}}{p}\cdot p\right)^2}{2p} + \ldots = \frac{a^{p-1}-1}{p}$$

не делится на p. Тогда в качестве n можно взять такое число, чтобы спаривание $\langle a, n\rangle_p$ стало бы равно 1 $(\mathrm{mod}\ p)$.
Действительно, так как НОД$(l(a), p) = 1$, то найдутся целые числа x и y такие, что $l(a)x + py = 1$. Заменяя, если нужно x на $x' = x + pk$, а y на $y' = y - l(a)k$, получаем, при подходящем k, что x' — натуральное число.

□

4.3.1 Формирование подписи

Алиса — доверенное лицо(арбитр). Она выбирает большое простое число p, взаимно простое с ним антивиферихово число $a \in \mathbb{Z}^{(p)}$ и $n \in \mathbb{N}^+$ такое, чтобы было выполнено сравнение

$$\langle a, n\rangle_p = \tfrac{a^{p-1}-1}{p} \cdot n \equiv 1 \pmod{p}.$$

Пусть x — случайное число такое, что $1 < x < p$, и s — решение сравнения $sx \equiv n \pmod{p}$.

Определение 4. *Набор (a, x, n) является секретным ключом.*

Пусть M $= \{m_1, m_2, \ldots, m_k\}$ — информация(сообщение). В криптографии определена функция, называемая хэш-функцией, которая однозначно задана информацией M.

Найдем остаток при делении a^{hx} на p^2:

$$r = a^{hx} \pmod{p^2},\ 0 < r < p^2.$$

Подписанное сообщение имеет вид $\prod = (\mathrm{M}, r < s < h)$. Получатель Боб должен проверить подпись, то есть проверить справедливость сравнения

$$\frac{r^{p-1}-1}{p} \cdot s \equiv h \pmod{p}, \tag{1}$$

то есть остаток $\frac{r^{p-1}}{p} \cdot s$ при делении на p должен быть равен ha.

Утверждение 2. *Если подпись верна, то сравнение (1) выполнено.*

Доказательство. Вычислим спаривание $\langle r, s \rangle_p$. Имеем

$$\langle r, s \rangle_p \equiv l(r) \cdot s \equiv \frac{\log(1+\frac{r^{p-1}-1}{p})}{p} \cdot s = \frac{r^{p-1}-1}{p} \cdot s \equiv h \pmod{p}.$$

Действительно, так как $r = a^{hx} \pmod{p^2}$, то

$$\langle r, s \rangle_p = \langle a^{hx}, s \rangle_p \equiv x \langle a^h, s \rangle_p \equiv \langle a^h, sx \rangle_p \equiv h \langle a, n \rangle_p \equiv h \pmod{p}.$$

□

Утверждение 3. *Подпись* $\prod$ *удовлетворяет требованиям к подписи, то есть*

1. *никто, кроме Алисы, не может подписать сообщение с ее подписью;*
2. *в случае конфликта Алисы с Бобом, они обращаются к третьим лицам, и судья проверяет подлинность подписи после предъявления ему чисел* (a, x, n).

5 Заключение

В данной работе рассмотрены криптографические примитивы шифрования и подписи, использующие основные понятия теории чисел. Предложен алгоритм электронной подписи, основанный на билинейном преобразовании использующем упрощенный вид спаривания в явном законе взаимности, описанный С. В. Востоковым в работе [2], где было дано окончательное решение 9-ой проблемы Гильберта.

Список используемой литературы

[1] А.А. Бухштаб, - Теория чисел, Москва, 1960

[2] С.В. Востоков, - Явная форма закона взаимности, Изв. АН СССР, Сер мат, том 42б № 6, 1978

[3] Н. Коблиц, - Курс теории чисел и криптографии, Москва, изд ТВП, 2001

[4] Б. Шнайер, - Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си, Москва, изд. Триумф, 2002

[5] Б. Шнайер, - Секреты и ложь. Безопасность данных в цифровом мире, изд. Питер, 2003

[6] R. Rivest, A. Shamir, L. Adleman, - A method for obtaining digital signatures and public key cryptosystems, Commum. ACM, vol. 21, no. 2, pp. 120-126, Feb. 1978