ПРОБЛЕМА ДИСКРЕТНОГО ЛОГАРИФМА И ПРОБЛЕМА ДИФФИ – ХЕЛЛМАНА

1 Введение

Пусть $G =< G; \cdot >$ – конечная группа, a и α – элементы группы G, n есть порядок элемента α. Натуральное число x называется *дискретным логарифмом элемента a при основании α*, если

$$\alpha^x = a, \ 0 \leq x \leq n.$$

Проблема дискретного логарифма заключается в том, что необходимо найти дискретный логарифм x данного элемента $a = \alpha^x$ при основании α.

Все известные вероятностные алгоритмы для решения этой проблемы (при подходяще выбранных группе и элементе α) субэкспоненциальны.

Вместо термина «дискретный логарифм элемента a при основании α» применяют термин «индекс элемента a при основании α». Далее в качестве группы рассматривается мультипликативная группа из ненулевых элементов конечного поля F_q. Если $q = p$, где p – простое число, а α есть образующий элемент этой группы, то определенное выше число x называют *индексом* числа a при основании α по модулю p.

Задача определения дискретного логарифма элемента при заданном основании в конечной мультипликативной группе не может быть решена методом последовательного приближения, метод полного перебора применим только для малых групп.

2 Алгоритм согласования

Теорема 2.2 *Пусть n, r – натуральные числа, $r^2 \geq n$. Для любого целого x можно указать целые числа s и t такие. что*

$$x \equiv sr + t \pmod{n}; 0 \leq s < r, \ 0 \leq t < r.$$

Доказательство. Можно предполагать, что $0 \leq x < n$. Полагаем

$$s = \left\lfloor \frac{x}{r} \right\rfloor, \ t = x - sr.$$

Имеем

$$0 \leq s \leq \frac{x}{r} < \frac{n}{r} \leq r.$$

С другой стороны,

$$0 \leq s \leq \frac{x}{r} < s + 1,$$

поэтому
$$sr \le x < sr + r,$$
или
$$0 \le x - sr = t < r.$$

Лемма 2.1. *Для вычисления степени m^n, где m – элемент некоторого кольца, а n – натуральное число, достаточно выполнить не более $2\lfloor \log_2 n \rfloor$ операций умножения.*

Доказательство. Пусть $2^{k-1} \le n < 2^k,\ k-1 = \lfloor \log_2 n \rfloor$. Тогда, представляя n в двоичной системе счисления, получим
$$n = e_0 + e_1 \cdot 2 + e_2 \cdot 2^2 + \ldots + e_{k-1} \cdot 2^{k-1} \le 1 + 2 + 4 + \ldots + 2^{k-1} = 2^k - 1 < 2^k,$$
$$m^n = m^{e_0} \cdot m^{e_1 \cdot 2} \cdot m^{e_2 \cdot 2^2} \cdot \ldots \cdot m^{e_{k-1} \cdot 2^{k-1}}.$$
Для вычисления степеней $1,\ m,\ m^2,\ m^4,\ \ldots,\ m^{e_{k-1} \cdot 2^{k-1}}$ достаточно выполнить $k-1$ умножений (возведений в квадрат). Для получения результата, некоторые из этих степеней надо перемножить, при этом будет выполнено не более $k-1$ умножений.

Теорема 2. 3. *Пусть $G =< G; \cdot >$ – конечная группа, a и α – элементы группы, n – порядок группы G;*
$$\alpha^x = a. \qquad (1)$$

Тогда число x можно найти, выполнив не более, чем $2(\sqrt{n} + \log_2 n) - 1$ операций умножения в группе G.

Доказательство. Полагаем $r = \lfloor \sqrt{n} \rfloor + 1$. Рассмотрим ряды
$$1,\ \alpha,\ \alpha^2\ \ldots,\ \alpha^{r-1},$$
$$a,\ a \cdot \alpha^{-1 \cdot r},\ a \cdot \alpha^{-2 \cdot r},\ \ldots,\ a \cdot \alpha^{-(r-1)r}.$$

Если $\alpha^x = a$ разрешимо относительно x, то по теореме 2.2 (учитывая, что $r^2 \ge n^2$) представим x в виде
$$x \equiv t + s \cdot r \pmod{n},\ 0 \le t < r.$$
Так как n кратно порядку элемента α, то $\alpha^x = \alpha^{sr+t} = a$ в том и только том случае, когда
$$\alpha^t = a \cdot \alpha^{-sr},$$
то есть когда найдётся элемент второго ряда, совпадающий с некоторым элементом первого ряда.

При вычислении элементов первого ряда потребуется выполнить не более $r-2$ умножений. Для вычисления $\alpha^{-r} = \alpha^{n-r}$ в силу леммы 2.1 потребуется выполнить не более $2\log_2 n$ умножений. Не более чем $r-1$ умножений потребуется для вычисления всех членов второго ряда.

Таким образом, общее число операций умножения для решения уравнения (1) не превосходит

$$2r-3+2\log_2 n \leq 2(\sqrt{n}+\log_2 n)-1.$$

Теорема 2.4. *Пусть* $G =< G; \cdot >$ *– конечная группа,* a *и* α *– элементы группы,* n *– порядок группы* G*;* $\alpha^x = a$*. И пусть кроме того число* n *– составное:*

$$n = r_1 \cdot r_2,$$

$$1 < r_1 < n,\ 1 < r_2 < n.$$

Тогда дискретный логарифм элемента a *по основанию* α *можно вычислить, выполнив не более чем*

$$2(\sqrt{r_1}+\sqrt{r_2})+6\log_2 r_1 r_2+\log_2 r_1-1$$

операций умножения.

Доказательство. Заметим, что любое целое число $x,\ 0 \leq x < n$ однозначно представляется в виде:

$$x = r_2 \cdot l_1 + m_1;\ l_1, m_1 \in Z,$$

$$0 \leq l_1 < r_1,\ 0 \leq m_1 < r_2.$$

Равенство $\alpha^x = a$ можно записать в виде

$$\alpha^{r_2 \cdot l_1 + m_1} = a. \qquad (2)$$

Возведем обе части этого равенства в степень r_1 и с учётом того, что $n = r_1 \cdot r_2$ и $\alpha^n = 1$, получим

$$\alpha^{r_1 \cdot m_1} = a^{r_1}.$$

Обозначив $\alpha_1 = \alpha^{r_1},\ a_1 = a^{r_1}$, подучим более удобное представление последнего равенства:

$$\alpha_1^{m_1} = a_1.$$

Легко проверить. что порядок α_1 не превышает r_2. По теореме 2.2 m_1 как дискретный логарифм a_1 по основанию α_1 можно вычислить, выполнив не более чем $2(\sqrt{r_2}+\log_2 r_2)-1$ операций умножения.

Умножая обе части равенства (2) на α^{-m_1}, получим

$$\alpha_2^{l_1} = a_2,$$

где $\alpha_2 = \alpha^{r_2},\ a_2 = a \cdot \alpha^{-m_1}$.

Аналогично предыдущему, l_1 можно вычислить при помощи не более чем за $2(\sqrt{r_1}+\log_2 r_1)-1$ операций умножения. Далее $\alpha_1,\ a_1,\ \alpha_2,\ a_2$ вычисляются соответственно не более чем за $2\log_2 r_1,\ 2\log_2 r_1,\ 2\log_2 r_2,\ 1+2\log_2 n = 1 + 2\log_2 r_1 + 2\log_2 r_2$ операций умножения.

3 Проблема Диффи–Хеллмана

Пусть $(G, \cdot)$ – мультипликативная группа высокого порядка, α – ее образующий элемент. Даны два элемента этой группы α^x и α^y, где x и y – натуральные числа. Проблема Диффи–Хеллмана состоит в том, чтобы найти элемент α^{xy}. Алгоритм ее решения без предварительного нахождения дискретных логарифмов указанных чисел при основании α не известен. В качестве группы G могут выступать, например, группы Z_p^* или $GF(p^n)^*,\ p \geq 2$.

4 История вопроса

Алгоритм теоремы 4.2 был открыт А.О.Гельфондом в 1962 году. Алгоритм теоремы 4.3 был описан В.И.Нечаевым в 1965 году. В 1972 году В.И.Нечаев установил, что среди детерминированный алгоритмов нет лучших в определённом смысле, чем алгоритмы, описанные в теоремах 4.2 и 4.3. В широко доступной литературе эти алгоритмы называют алгоритмами Силвера-Поллига-Хеллмана. Продолжаются исследования других, недетерминированный алгоритмов.

Проблема Диффи–Хеллмана изучается в связи с протоколом распределения ключей для классической криптосистемы, предложенного в 1976 году американскими математиками Диффи и Хеллманом. Классическая версия этого протокола основана на проблеме Диффи–Хеллмана для группы Z_p^* Абоненты A и B, предварительно по открытому каналу обуславливают использовании большого простого числа p и образующего элемента α мультипликативной группы Z_p^*. Для совместной выработки секретной точки они выбирают независимо друг от друга секретные числа $x \in Z_p^*$ и $y \in Z_p^*$, вычисляют «половинки» α^x и α^y и обмениваются ими по открытому каналу. После этого каждый из них вычисляет секретный ключ, возводя полученную «половинку» ключа в свою секретную степень: $(\alpha^x)^y = \alpha^{xy},\ (\alpha^y)^x = \alpha^{yx} = \alpha^{xy}$.

Аддитивный вариант проблемы дискретного логарифма и аддитивная интерпретация алгоритма согласования излагаются в монографии [1].

5 Контрольные вопросы

1. Сформулируйте проблему дискретного логарифмирования.

2. Почему для дискретного логарифмирования неприменим метод логарифмирования на числовой оси?

3. Какое тождество лежит в основе алгоритма согласования для вычисления дискретного логарифма.

4. Почему дискретный логарифм можно легко вычислить,если порядок группы не содержит большой простой множитель?

5. (Факультативно) Сформулируйте аддитивный вариант алгоритма согласования применительно к группе точек эллиптической кривой (см. [2]).

Литература.

1. Болотов А.А., Гашков С.Б., фролов А.Б. Элементарное введение в эллиптическую крипторафию. Протоколы криптографии на эллиптических кривых. – М: Комкнига, 2006.

2. О. Василенко. Теоретико-числовые алгоритмы в криптографии. М:МЦНМО. 2004.

3. В.И.Нечаев. Защита информации. Основы криптографии.М: Высшая школа. 1999.