CRYPTOGRAPHY

МАТЕМАТИЧНІ ОСНОВИ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ

Лек. 4   2021 КІБ-18

МОДУЛЬНАЯ АРИФМЕТИКА # 2

Диофантово уравнение.

- **В общем виде**

$$F(a_1, a_2, \dots, a_n, x_1, x_2, \dots, x_m) = 0$$

где a_i , x_j - целые!

- **Линейное**

$$a_1 * x_1 + a_2 * x_2 + \cdots a_n * x_n = b$$

- **Линейное с 2-мя переменными**

$$a * x + b * y = c \qquad (1)$$

Все a, b, c, x, y целые !!!
Важно! Если gcd(*a*,*b*) $\nmid$ *c* – уравнение неразрешимо в целых.
Важно! Если gcd(*a*,*b*) | *c* – уравнение разрешимо в целых. Имеет бесконечное число решений.

Линейное диофантово уравнение

Пусть gcd(*a*,*b*) = *d* и *d* | *c* *(бесконечное число решений)* ,
тогда (1) , делим на *d*

$$a_1 x + b_1 y = c_1$$

Находим параметры s, t в равенстве (используем расширенный алгоритм Эвклида)

$$a_1 s + b_1 t = 1$$

Тогда частное решение

$$x_0 = \frac{c}{d} s, \qquad y_0 = \frac{c}{d} t$$

Общее решение

$$x = x_0 + k\frac{b}{d}, \qquad y = y_0 - k\frac{a}{d}$$

где *k* - целое.

Линейное диофантово уравнение

Решить

$$21x + 14y = 35$$

1. $\gcd(21, 14) = 7$, $d = 7$
2. $7 \mid 35 = \text{true}!$ **Бесконечное число решений**
3. $3x + 2y = 5 \quad \rightarrow$ решаем $3s + 2t = 1$
4. **Используем алгоритм Эвклида**
5. $$s = 1, t = -1$$

Частное решение

$$x_0 = \frac{35}{7} * 1 = 5, \qquad y_0 = \frac{35}{7} * -1 = -5$$

Общее решение $x = 5 \quad + 2k, \quad y = -5 \quad - 3k$

Частное решение при $k = 2 \rightarrow x = 9, y = -11$

Линейное уравнение с одним неизвестным, содержащее сравнение

~~*Уравнение 1-го порядка*~~ $ax = b$

Уравнение вида

$$ax \equiv b \pmod{n}$$

a, b, n - **заданные целые!**

Например: $125x \equiv 11 \pmod{15}$

Например: $125x \equiv 10 \pmod{15}$

Может :

а) не иметь решения

б) ограниченное число решений.

Пусть $d = gcd(a, n)$

Тогда

а) если $d \nmid b$ **- нет решения**

б) если $d | b$ **- есть** d **решений**

Линейное уравнение с одним неизвестным, содержащее сравнение

Уравнение вида

$$a\,x \equiv b\ (mod\ n)$$

Алгоритм решения:

а) сокращаем уравнение – делим на d

б) умножаем обе стороны на мультипликативную инверсию $\left(\frac{a}{d}\right)^{-1}$ – находим решение x_0.

Общее решение имеет вид

$$x = x_0 + k * \frac{n}{d}, \qquad k = 0, 1, \dots, (d-1)$$

Линейное уравнение с одним неизвестным, содержащее сравнение

Пример.

$$125\,x \equiv 10\ (mod\ 15)$$

Находим $d = gcd(125, 15) = 5$ → делит

Сокращаем на $d = 5$

$$25\,x \equiv 2\ (mod\ 3)$$

Или

$x_0 \equiv 2 * 25^{-1}\ (mod\ 3)$ $\quad , \rightarrow 25^{-1}\ (mod\ 3) = 1$

То есть $x_0 \equiv 2 * 1\ (mod\ 3) = 2$

Общее решение имеет вид

$$x = 2 + k * 3, \qquad k = 0, 1, 2$$

$$x_0 = 2;\ x_1 = 5\ ;\ x_2 = 8\ ;$$

Линейное уравнение с одним неизвестным, содержащее сравнение

Пример.

$$14\,x \equiv 12\ (mod\ 18)$$

Находим $d = gcd(14, 18) = 2$ → делит

Сокращаем на $d = 2$

$$7\,x \equiv 6\ (mod\ 9)$$

Или

$x_0 \equiv 6 * 7^{-1}\ (mod\ 9)$, $\rightarrow 7^{-1}\ (mod\ 9) = 4$

То есть $x_0 \equiv 6 * 4\ (mod\ 9) = 6$

Общее решение имеет вид

$$x = 6 + k * 9, \qquad k = 0, 1$$

Линейное уравнение с одним неизвестным, содержащее сравнение

Пример.

$$7x \equiv 9 \ (mod\ 13)$$

Находим $d = gcd(7, 13) = 1$ → делит

Сокращаем на $d = 1$

$$7x \equiv 9 \ (mod\ 13)$$

Или

$$x_0 \equiv 9 * 7^{-1} \ (mod\ 13) \quad , \rightarrow 7^{-1} \ (mod\ 13) = 2$$

То есть $x \equiv 9 * 2 \ (mod\ 13) = 18 \ (mod\ 13) = 5$

Общее решение имеет вид

$$x = 5$$

Система линейных алгебраических уравнений (СЛАУ)

Стандартная СЛАУ $A * X = B$ **или**

$$\begin{pmatrix} a_{1,1} & \cdots & a_{1,m} \\ \vdots & \ddots & \vdots \\ a_{m,1} & \cdots & a_{m,m} \end{pmatrix} * \begin{bmatrix} x_1 \\ \vdots \\ x_m \end{bmatrix} = \begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix}$$

Если $det(A) \neq 0$ есть A^{-1}и $X = A^{-1}B$.

Обратная матрица A^{-1} ищется как

$$A^{-1} = \frac{1}{det(A)} A^*,$$

где A^* транспонированя матрица *алгебраических дополнений* $a^*_{j,i} = (-1)^{i+j} * M_{i,j}$, ($M_{i,j}$ - минор).

Система линейных уравнений, содержащих сравнения

Уравнение вида

$$A * X \equiv B \pmod{n}$$

или

$$\begin{pmatrix} a_{1,1} & \cdots & a_{1,m} \\ \vdots & \ddots & \vdots \\ a_{m,1} & \cdots & a_{m,m} \end{pmatrix} * \begin{bmatrix} x_1 \\ \vdots \\ x_m \end{bmatrix} \equiv \begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix} \pmod{n}$$

? если есть A^{-1} **мультипликативная** инверсия матрицы A, то

$$X \equiv A^{-1}B \pmod{n}$$

Множество $\mathbb{R}$

1 порядок	n-й порядок
$a * x = b$	$A * X = B$
$x = a^{-1}b$	$X = A^{-1}B$

Множество $\mathbb{Z}_n$

1 порядок	n-й порядок
$a * x \equiv b \ (mod\ n)$	$A * X \equiv B \ (mod\ n)$
$x \equiv a^{-1}b \ (mod\ n)$	$X \equiv A^{-1}B \ (mod\ n)$

Матрицы в $\mathbb{Z}_n$. Матрицы вычетов

Особенность:

Мультипликативная инверсия матриц:

матрица A, где все $a_{i,j} \in \mathbb{Z}_n$, имеет мультипликативную инверсию, только если $\mathbf{det}(A)$ имеет мультипликативную инверсию в $\mathbb{Z}_n$.

Например:

$$A = \begin{matrix} 7 & 4 \\ 1 & 5 \end{matrix}, \qquad n = 10$$

$$\det(A) = 7 * 5 - 4 * 1 = 31$$

$$\det(A) mod 10 = 1 \ \ !!!!! \ \ \det(\mathrm{A})^{-1} = 1$$

Матрицы в $\mathbb{Z}_n$. Мультипликативная инверсия матрицы. Пример

Последовательность поиска инверсной матрицы.

Пусть $[\boldsymbol{det}(\boldsymbol{A})]^{-1}$ **в** $\mathbb{Z}_n$ **есть !** и найдены все алгебраические дополнения $a^*_{j,i}$.

Для каждого ***i,j*** решаем линейное уравнение

$$det\,(A) * \boldsymbol{a}^{-1}_{j,i} \equiv a^*_{j,i}(\boldsymbol{mod}\,\boldsymbol{n})$$

Таким образом формируется матрица $(\boldsymbol{A})^{-1}$

Матрицы в $\mathbb{Z}_n$. Мультипликативная инверсия матрицы. Пример

Дана A в $\mathbb{Z}_{10}$

$$A = \begin{matrix} 7 & 4 \\ 1 & 5 \end{matrix}, \; det(A) = 1 \;, ?\, B = \begin{matrix} 6 \\ 3 \end{matrix}.$$

Ищем мультипликативную инверсию **1** в $\mathbb{Z}_{10}$.

Находим $gcd(26, 21) = 1$.

$$det(A)^{-1}\, mod\, 1 = 1$$

$$A^{-1} = \begin{bmatrix} 5mod10 & -4mod10 \\ -1mod10 & 7mod10 \end{bmatrix} = \begin{bmatrix} 5 & 6 \\ 9 & 7 \end{bmatrix}$$

$$X = \begin{bmatrix} (5*6+6*3)mod10 \\ (9*6+7*3)mod10 \end{bmatrix} = \begin{bmatrix} 48mod10 \\ 75mod10 \end{bmatrix} = \begin{bmatrix} 8 \\ 5 \end{bmatrix}$$

$$X = \begin{bmatrix} 8 \\ 5 \end{bmatrix}$$

Матрицы в $\mathbb{Z}_n$. Мультипликативная инверсия матрицы. Пример

Дана A в $\mathbb{Z}_{26}$

$$A = \begin{bmatrix} 3 & 5 & 7 & 2 \\ 1 & 4 & 7 & 2 \\ 6 & 3 & 9 & 17 \\ 13 & 5 & 4 & 16 \end{bmatrix}, \; det(A) = 21 .$$

Ищем мультипликативную инверсию 21 в $\mathbb{Z}_{26}$ (расширенный алгоритм Эвклида).

Находим $gcd(26, 21) = 1$ и $t = 5$.

$$det(A)^{-1} \, mod \, 26 = 5$$

Матрицы в $\mathbb{Z}_n$. Мультипликативная инверсия матрицы. Пример

Решение

$$A^{-1} = \begin{bmatrix} 15 & 21 & 0 & 15 \\ 23 & 9 & 0 & 22 \\ 15 & 16 & 18 & 3 \\ 24 & 7 & 15 & 3 \end{bmatrix}$$

Вопросы:

- Укажите условие существования решения уравнения $\boldsymbol{a * x + b * y = c}$ и опишите порядок поиска решения.
- Укажите условие существования решения уравнения $\boldsymbol{a\,x \equiv b\ (mod\ n)}$ и опишите порядок поиска решения.
- Как найти мультипликативно инверсную матрицу в $\mathbb{Z}_{\boldsymbol{n}}$?

ЛИТЕРАТУРА

Нечаев В.И. Элементы криптографии (Основы теории защиты информации).- Учеб. пособие. – М.:, ВШ., 1999.- 109 с.

Введение в криптографию. **Под общ. ред. В.В.Ященко.** – 4-е изд., доп. М.: МЦНМО, 2012 – 348 с. ISBN 978-5-4439-0026-1

ЛИТЕРАТУРА

Венбо Мао. Современная криптография: теория и практика.—М.: Издательский дом «Вильямс», 2005.—768 с.: ил. ISSN 5-8459-0847-7 (рус.)

Шнайер Б. Прикладная криптография. Протоколы, алгоритмы и исходный код на Си. – Москва: Вильямс, 2016. 1024 с.

ЛИТЕРАТУРА

Francisco Rodriguez-Henriquez, N.A. Saqib, A. Diaz-Perez, Cetin Kaya Koc.

Cryptographic Algorithms on Reconfigurable Hardware. - Springer, 2006.

A. Menezes, P. van Oorschot, S. Vanstone.

Handbook of Applied Cryptography.- CRC Press, 1996.

END # 4