Авдошин С.М., Савельева А.А.

Алгоритм решения систем линейных уравнений в кольцах вычетов

Разработан эффективный алгоритм решения систем линейных уравнений в кольцах вычетов [1], эквивалентный по сложности известному алгоритму решения систем в полях Галуа ([2], [4]). Приведены результаты сравнительного анализа предложенного алгоритма и существующих аналогов ([3], [10], [8]) на основе асимптотической оценки их временной сложности. Показано, что разработанный метод является корректным и существенно снижает трудоемкость алгоритмов дискретного логарифмирования.

Введение

Объектом исследования данной работы являются методы решения систем линейных уравнений в кольцах вычетов. Такие системы возникают в алгоритмах факторизации и дискретного логарифмирования (см., например, метод Диксона, алгоритм Копперсмита-Одлыжко-Шреппеля «COS» и алгоритм решета числового поля в [3]).

Частным случаем колец вычетов являются поля Галуа, т.е. кольца вычетов по модулю простых чисел. Методы решения систем в таких полях известны (см., например, метод Гаусса (последовательного исключения) в [2, с.89], [4, с.42]). Модификацией метода Гаусса является метод Жордана. Однако для решения систем линейных уравнений в кольцах вычетов эти методы, вообще говоря, неприменимы.

Проиллюстрируем сказанное. Рассмотрим систему линейных уравнений:

$$\begin{cases} 26x + \ \ 3y = 4 \\ \ \ 9x + 34y = 1 \end{cases} \qquad (1)$$

в поле Галуа $\mathbb{Z}_{37}$ и в кольце вычетов $\mathbb{Z}_{36}$.

В соответствии с методом Жордана требуется с помощью элементарных преобразований над строками привести матрицу к единичной. Для получения единичного элемента на диагонали в поле действительных чисел используется деление на число a, равное ведущему элементу; аналогом этой операции в кольце вычетов является умножение на элемент, обратный к a. Обратный элемент по модулю p можно найти как решение уравнения:

$$ax \equiv 1 (\operatorname{mod} p) \qquad (2)$$

Для его вычисления используется расширенный алгоритм Евклида (см. [7, с. 744], [10, с.227]). На рис.1 приведено описание этого алгоритма. Если a и p - взаимно простые числа, т.е. $НОД(a,p) = 1 = a \cdot x + p \cdot y$, то коэффициент Безу x является решением уравнения (2); в противном случае уравнение (2) не имеет решения и элемент a необратим в кольце $\mathbb{Z}_p$.

Как показано в [7, с.743], время работы алгоритма Евклида при вычислении $НОД(a,b)$, где $a > b \geq 0$, составляет $O(\log b)$. Тогда сложность операции вычисления обратного элемента в кольце $\mathbb{Z}_p$ можно оценить как $O(\log p)$. Метод Жордана с учетом алгоритма Евклида имеет временную сложность $O\left(n\cdot(n\cdot m+\log p)\right)$ для системы n уравнений с m неизвестными в $\mathbb{Z}_p$.

Евклид(a, b)

1. $\begin{pmatrix} d & x & y \\ n & r & s \end{pmatrix} \leftarrow \begin{pmatrix} a & 1 & 0 \\ b & 0 & 1 \end{pmatrix}$
2. $c \leftarrow \lfloor d/n \rfloor$
3. $\begin{pmatrix} d & x & y \\ n & r & s \end{pmatrix} \leftarrow \begin{pmatrix} 0 & 1 \\ 1 & -c \end{pmatrix} \times \begin{pmatrix} d & x & y \\ n & r & s \end{pmatrix}$
4. *ЕСЛИ* $n > 0$
5. | *ТО* перейти к шагу 2;
6. | *ИНАЧЕ* вернуть (d, x, y, r, s)

Рис.1

В результате вычислений, приведенных ниже, получаем решение системы в поле Галуа $\mathbb{Z}_{37}$: $x=16,\ y=23$.

$$\begin{matrix}[1]\\ [2]\end{matrix}\left(\begin{array}{cc|c} 26 & 3 & 4 \\ 9 & 34 & 1 \end{array}\right) \xrightarrow{[1]\cdot\left(26^{-1}=10\right)} \left(\begin{array}{cc|c} 1 & 30 & 3 \\ 9 & 34 & 1 \end{array}\right) \xrightarrow{[2]-[1]\cdot 9} \left(\begin{array}{cc|c} 1 & 30 & 3 \\ 0 & 23 & 11 \end{array}\right)$$

$$\begin{matrix}[1]\\ [2]\end{matrix}\left(\begin{array}{cc|c} 1 & 30 & 3 \\ 0 & 23 & 11 \end{array}\right) \xrightarrow{[2]\cdot\left(23^{-1}=29\right)} \left(\begin{array}{cc|c} 1 & 30 & 3 \\ 0 & 1 & 23 \end{array}\right) \xrightarrow{[1]-[2]\cdot 30} \left(\begin{array}{cc|c} 1 & 0 & 16 \\ 0 & 1 & 23 \end{array}\right)$$

Однако в кольце вычетов по модулю $p=36$ система (1) не может быть решена ни с помощью метода Жордана, ни с помощью метода Гаусса, поскольку все коэффициенты при неизвестных являются делителями нуля ([9, с.75]) и, следовательно, не является обратимыми. Таким образом, получить единичный элемент на диагонали умножением на какой-либо элемент кольца невозможно.

Тем не менее, конечность области определения позволяет убедиться в том, что решение данной системы в $\mathbb{Z}_{36}$ существует $(x=17,\ y=22)$, и притом единственно.

Для решения систем линейных уравнений в кольцах вычетов необходимы специальные методы.

<u>Обзор существующих методов</u>

Анализ методов решения систем линейных уравнений в кольцах вычетов, описанных в современной литературе, выявил ряд недостатков, которые затрудняют использование этих алгоритмов на практике.

В монографии [3] задача сводится к решению систем линейных уравнений над полями Галуа. Пусть

$$\sum_{j=1}^{m} a_{ij} x_j \equiv b_i (\operatorname{mod} p), \qquad i = \overline{1,n} \tag{3}$$

где $p = \prod_{k=1}^{t} q_k^{\alpha_k}$, тогда решение системы (3) сводится к решению семейства систем

$$\sum_{j=1}^{m} a_{ij} x_j \equiv b_i (\operatorname{mod} q_k^{\alpha_k}), \qquad i = \overline{1,n}, \quad k = \overline{1,t} \tag{4}$$

где неизвестные значения $x_j (\operatorname{mod} q_k^{\alpha_k})$ для фиксированного k представляются в виде

$$x_j \equiv x_{j0} + x_{j1} q_k + \ldots + x_{j,\alpha_k - 1} q_k^{\alpha_k - 1} \ (\operatorname{mod} q_k^{\alpha_k}), \tag{5}$$

Здесь $0 \le x_{jl} \le q_k - 1, \quad l = \overline{0, \alpha_k - 1}$.

Редуцируя систему (4) к модулю q_k, получаем систему уравнений:

$$\sum_{j=1}^{m} a_{ij} x_{j0} \equiv b_j (\operatorname{mod} q_k), \qquad i = \overline{1,n}$$

над полем Галуа $\mathbb{Z}_{q_k}$. Если мы найдем все $x_{j0}, \quad j = \overline{1,m}$, то, подставляя x_j в виде (5) с известными x_{i0} в систему (4), редуцируя ее к модулю q_k^2 и затем поделив на q_k, мы получим систему линейных уравнений над полем $\mathbb{Z}_{q_k}$ относительно неизвестных $x_{j1}, \quad j = \overline{1,m}$, и т.д. В конечном счете, найдя значение $x_j (\operatorname{mod} q_k^{\alpha_k})$ для всех k, мы восстановим $x_j (\operatorname{mod} p)$ по китайской теореме об остатках (см. [10, с.420]).

В нашем примере $p = 36 = 2^2 \cdot 3^2$, т.е. для решения одной системы в кольце вычетов придется решить 4 системы над полями Галуа. Но основным недостатком метода является необходимость разложения на множители числа p: вопрос о существовании алгоритма факторизации с полиномиальной сложностью является одной из открытых проблем современной теории чисел.

Другой метод предполагает сведение системы линейных уравнений в кольце вычетов к системе линейных диофантовых уравнений. При помощи одного из известных алгоритмов (см. [3] или [10]) расширенная матрица системы $(A \mid b)$ приводится к *ступенчатому виду* $(A' \mid b')$ и вычисляется *правая матрица перехода* R размером $(m+1) \times (m+1)$, такая, что: $(A \mid b) \times R = (A' \mid b')$. На основании матрицы R можно получить общее решение системы.

Проиллюстрируем применение данного способа на примере. Система линейных диофантовых уравнений, соответствующая системе (1) в $\mathbb{Z}_{36}$, имеет вид:

$$\begin{cases} 26x + \ \ 3y + 36v_1 \qquad\quad = 4 \\ \ \ 9x + 34y \qquad\quad + 36v_2 = 1 \end{cases}.$$

Ее общее решение в кольце целых чисел:

$$\begin{cases} x = \ \ 5653025 \ + \ t_0 \cdot 1224 \ \ + \ t_1 \cdot (\text{-}21492) \\ y = \ \text{-}1496390 \ + \ t_0 \cdot (\text{-}324) \ + \ t_1 \cdot 5688 \\ v_1 = \text{-}3958042 \ + \ t_0 \cdot (\text{-}857) \ + \ t_1 \cdot 15048 \\ v_2 = \qquad\quad 0 \ + \ t_0 \cdot 0 \ \ + \ \ t_1 \cdot 1 \end{cases} , \quad t_0, t_1 \in \mathbb{Z}$$

Редуцируя результат к модулю 36, получаем: $x = 17,\ y = 22$.

Однако при решении систем линейных уравнений в кольцах вычетов наблюдается экспоненциальный рост длины коэффициентов. Так, в нашем примере коэффициенты исходной матрицы ограничены числом 36, тогда как в целых числах мы получили общее решение с коэффициентами ~ 10^6. Заметим, что этот результат соответствует системе в кольце вычетов, состоящей всего лишь из двух уравнений с двумя неизвестными.

Для того, чтобы избежать экспоненциального роста длины коэффициентов, разработаны специальные методы решения систем линейных алгебраических уравнений над кольцом целых чисел, такие как модификация метода Гаусса и построение нормальной диагональной формы Смита (см. [8, с. 81]). Несмотря на то, что эти алгоритмы являются полиномиальными, их сложность существенно превышает сложность алгоритма Гаусса при решении систем в полях Галуа. Так, для системы из n уравнений с n неизвестными, коэффициенты которой по абсолютной величине не превосходят α, временная сложность модифицированного алгоритма Гаусса при использовании самого быстрого алгоритма умножения составляет $O\left(n^4(\log\alpha + \log n)\right)$. Трудоемкость построения нормальной диагональной формы Смита матрицы $A_{n\times m}$, где $|a_{ij}| \le \alpha, i = \overline{1,n},\ j = \overline{1,m}$, ограничена величиной $O\left(n^2 m^2 \log\alpha\right)$.

Метод решения систем линейных уравнений в кольцах вычетов, предлагаемый в данной работе, лишен недостатков вышеописанных алгоритмов и показал свою эффективность при программной реализации.

Описание метода

В основе разработанного метода лежит преобразование строк матрицы с использованием коэффициентов Безу, которые позволяет вычислить расширенный алгоритм Евклида (см. рис.1). В результате работы алгоритма получаем:

$$НОД(a,b) = d = a \cdot x + b \cdot y,$$

$$0 = n = a \cdot r + b \cdot s.$$

При $a = 26 = a_{11},\ b = 9 = a_{21}$:

$$НОД(26,9) = 1 = 26 \cdot (-1) + 9 \cdot (3),$$

$$0 = 26 \cdot (9) + 9 \cdot (-26).$$

Применяя к 1-й и 2-й строке расширенной матрицы системы (1) преобразования, соответствующие преобразованиям алгоритма Евклида над поступающими на его вход коэффициентами $a_{11} = 26$ и $a_{21} = 9$, в результате мы получаем матрицу, строчно эквивалентную исходной (см. [5, с.127]):

$$\begin{array}{c} [1] \\ [2] \end{array} \left(\begin{array}{cc|c} 26 & 3 & 4 \\ 9 & 34 & 1 \end{array}\right) \xrightarrow{[1]-[2]\cdot 2} \left(\begin{array}{cc|c} 8 & 7 & 2 \\ 9 & 34 & 1 \end{array}\right) \xrightarrow{[1]\leftrightarrow[2]} \left(\begin{array}{cc|c} 9 & 34 & 1 \\ 8 & 7 & 2 \end{array}\right)$$

$$\begin{array}{c} [1] \\ [2] \end{array} \left(\begin{array}{cc|c} 9 & 34 & 1 \\ 8 & 7 & 2 \end{array}\right) \xrightarrow{[1]-[2]\cdot 1} \left(\begin{array}{cc|c} 1 & 27 & 35 \\ 8 & 7 & 2 \end{array}\right) \xrightarrow{[1]\leftrightarrow[2]} \left(\begin{array}{cc|c} 8 & 7 & 2 \\ 1 & 27 & 35 \end{array}\right) \qquad (6)$$

$$\begin{array}{c} [1] \\ [2] \end{array} \left(\begin{array}{cc|c} 8 & 7 & 2 \\ 1 & 27 & 35 \end{array}\right) \xrightarrow{[1]-[2]\cdot 8} \left(\begin{array}{cc|c} 0 & 7 & 10 \\ 1 & 27 & 35 \end{array}\right) \xrightarrow{[1]\leftrightarrow[2]} \left(\begin{array}{cc|c} 1 & 27 & 35 \\ 0 & 7 & 10 \end{array}\right)$$

В полученной матрице:

$$\begin{pmatrix} A(1,*) \\ A(2,*) \end{pmatrix} = \begin{pmatrix} x' & y' \\ r' & s' \end{pmatrix} \times \begin{pmatrix} A(1,*) \\ A(2,*) \end{pmatrix},$$

где x', y', r', s' удовлетворяют условию: $НОД(a_{11}, a_{21}) = a_{11} \cdot x' + a_{21} \cdot y'$, $0 = a_{11} \cdot r' + a_{21} \cdot s'$ (запись $A(k,*)$ используется для обозначения k-й строки расширенной матрицы A). Коэффициенты Безу $x' = -1, y' = 3, r' = 9, s' = -26$ можно получить, оперируя лишь коэффициентами a_{11} и a_{21}. Тогда цепь преобразований (6) сводится к одному преобразованию следующего вида:

$$\begin{array}{c} [1] \\ [2] \end{array} \left(\begin{array}{cc|c} 26 & 3 & 4 \\ 9 & 34 & 1 \end{array}\right) \xrightarrow[{[2]'=[1]\cdot 9+[2]\cdot 10}]{[1]'=[1]\cdot 35+[2]\cdot 3} \left(\begin{array}{cc|c} 1 & 27 & 35 \\ 0 & 7 & 10 \end{array}\right)$$

С учетом того, что коэффициент $a_{22} = 7$ обратим в $\mathbb{Z}_{36}$: $7^{-1} \equiv 31 (\bmod 36)$, преобразуем матрицу к единичной и получаем решение:

$$\begin{array}{c} [1] \\ [2] \end{array} \left(\begin{array}{cc|c} 1 & 27 & 35 \\ 0 & 7 & 10 \end{array}\right) \xrightarrow[{[2]'=[2]\cdot 31}]{[1]'=[1]+[2]\cdot 27} \left(\begin{array}{cc|c} 1 & 0 & 17 \\ 0 & 1 & 22 \end{array}\right)$$

В общем виде алгоритм решения систем линейных уравнений в кольцах вычетов, представляющий собой модификацию метода Жордана, описан на рис.2.

Доказательство корректности

Предложенный алгоритм является корректным, т.е. полученная в результате преобразований система равносильна исходной (иначе говоря, решения системы не теряются и новые решения не появляются).

Запишем систему уравнений (3) в матричном виде:

$$Ax = b \qquad (7)$$

Тогда по теореме о равносильности систем линейных уравнений**:**

Если U *- обратимая* $(n \times n)$*-матрица над* R (R *- произвольное коммутативное кольцо с единицей*), *тогда система уравнений* (7) *равносильна системе* $(UA)x = Ub$.

(Доказательство см. в [5, с.158]).

Следствие из этой теоремы:

Если матрицы (A, b) *и* (C, δ) *строчно эквивалентны*, *то система уравнений* (7) *равносильна системе* $Cx = \delta$.

Поскольку преобразования матрицы в описанном модифицированном методе Жордана базируются на элементарных преобразованиях строк (*элементарными преобразованиями строк матрицы* с элементами из коммутативного кольца с единицей называют (см. [6, с.85]) умножение любой ее строки на обратимый элемент кольца; прибавление к любой ее строке другой строки, умноженной на произвольный элемент кольца; транспозицию строк), то полученная на выходе алгоритма матрица строчно эквивалентна исходной (см.

$\textit{Модиф\_Жордан}(A)$

1. $n \leftarrow \textit{Число\_Строк}(A)$
2. $i \leftarrow 1$
3. *ДЛЯ* $j = \overline{i+1, n}$ *ЦИКЛ*
4. | *ВЫЧИСЛИТЬ* $x', y', r', s' : \left\{ \begin{matrix} \textit{НОД}(a_{ii}, a_{ji}) = a_{ii} \cdot x' + a_{ji} \cdot y' \\ 0 = a_{ii} \cdot r' + a_{ji} \cdot s' \end{matrix} \right\}$
5. | $\begin{pmatrix} A(i,*) \\ A(j,*) \end{pmatrix} \leftarrow \begin{pmatrix} x' & y' \\ r' & s' \end{pmatrix} \times \begin{pmatrix} A(i,*) \\ A(j,*) \end{pmatrix}$
6. *ЕСЛИ* коэффициент a_{ii} необратим в $\mathbb{Z}_p$
7. | *ТО* выйти из алгоритма {*матрица вырождена*}
8. | *ИНАЧЕ* {*обнуляем все элементы* i *–го столбца выше ведущего*}
9. | | $A(i,*) \leftarrow A(i,*) \cdot a_{ii}^{-1}$
10. | | $A(j,*) \leftarrow A(j,*) - A(i,*) \cdot a_{ji}, \quad j = \overline{1, i-1}$
11. $i \leftarrow i+1$
12. *ЕСЛИ* $i \le n$
13. | *ТО* перейти к шагу 2;
14. | *ИНАЧЕ* вернуть(A)

Рис.2

[5, с.127]). Тогда приведенному выше следствию соответствующие системы уравнений являются равносильными. Что и требовалось доказать.

<u>Оценка сложности</u>

Предложенный алгоритм обладает временной сложностью $O\left(n \cdot (nm + \log p)\right)$ для системы в кольце вычетов по модулю p, в которой n - число уравнений системы, m - число неизвестных.

Для получения этой формулы воспользуемся оценкой временной сложности алгоритма Евклида $T(a, b) = O\left(1 + \log_{\varphi} \dfrac{b}{\textit{НОД}(a, b)}\right)$, где $a > b \ge 0,\ \varphi = (1+\sqrt{5})/2$ (доказательство этой оценки предлагается в [7, с.745], в качестве упражнения).

На каждом j-м шаге процедура, реализующая алгоритм Евклида, вызывается j раз: первым параметром является текущее значение ведущего элемента, в качестве второго на вход последовательно подаются $a_{ij}\ (i=\overline{j+1,\, n})$ и p. Пусть d_i - значение ведущего элемента на i-й итерации цикла:

$$d_0 = a_{jj},\ d_1 = НОД(a_{jj},\, a_{j+1,j}) = НОД(d_0,\, a_{j+1,j}),\ \dots,$$
$$d_k = НОД(d_{k-1},\, a_{j+k,j}),\ \dots,\ d_{n-j} = НОД(d_{n-j-1},\, a_{n,j}).$$

Тогда число операций оценивается неравенством:

$$\sum_{i=1}^{n-j}\left(1+\log\frac{\min\left\{d_{i-1},\, a_{i,j}\right\}}{НОД(d_{i-1},\, a_{i,j})}\right) \le (n-j)+\log p.$$

Помимо этого, на каждом j-м шаге над элементами матрицы производится порядка $2(n-1)(m+1)\cong 2nm$ операций. Число шагов алгоритма для системы равно n. Получаем временную сложность алгоритма:

$$T(n,\, p) = \sum_{j=1}^{n}\left(2nm+(n-j)+\log p\right) \cong O\left(n\cdot(nm+\log p)\right).$$

<u>Заключение</u>

В заключение приведем сравнительный анализ временной сложности предложенного алгоритма и алгоритмов, описанных в современной литературе, для системы n уравнений с m неизвестными в кольце вычетов $\mathbb{Z}_p$ ($p=\prod_{k=1}^{t} q_k^{\alpha_k}$).

Алгоритм	Временная сложность
Модифицированный метод Жордана	$O\left(n\cdot(nm+\log p)\right)$
Метод сведения к полям Галуа*	$O\left(n\cdot(n\cdot m\cdot\sum_{k=1}^{t}\alpha_k+\log p)+\sqrt{\ln p\ln\ln p}\cdot e^{\sqrt{\ln p\ln\ln p}}\right)$
Метод сведения к диофантовым уравнениям (с построением матрицы Смита)	$O\left(n^2 m^2\log p\right)$

*Оценка временной сложности этого метода дана при условии использования для разложения на множители числа p наиболее эффективного на сегодняшний день (см. [7, с.779]) алгоритма «квадратичного решета» Померанца, имеющего временную сложность $L(p)^{1+o(1)}$, где $L(p)=e^{\sqrt{\ln p\ln\ln p}}$.

<u>**Список литературы**</u>

1. **Авдошин С.М., Савельева А.А.** Свидетельство об официальной регистрации программы для ЭВМ № 2005612258: «Программа решения систем линейных уравнений в кольцах вычетов». Зарегистрировано в Реестре программ для ЭВМ 02.09.2005.
2. **Ван дер Варден Б.Л**. Алгебра. - М.: Наука, 1976. - 623 с.
3. **Василенко О.Н.** Теоретико-числовые алгоритмы в криптографии. М.: МЦНМО, 2004. - 328 с.
4. **Гантмахер Ф.Р.** Теория матриц. Гостехиздат, 1953. - 576 с.
5. **Глухов М.М., Елизаров В.П., Нечаев А.А**. Алгебра: Учебник. В 2-х т. Т. I - М.: Гелиос АРВ, 2003. - 336с.
6. **Джекобсон Н.** Теория колец (Перевод с английского Н. Я. Виленкина). М.: Государственное издательство иностранной литературы, 1947. - 287 с.
7. **Кормен Т., Лейзерсон Ч., Ривест Р.** Алгоритмы: построение и анализ. М.: МЦНМО, 1999. - 960 с.
8. **Кузнецов М.И., Бурланков Д.Е., Чирков А.Ю., Яковлев В.А.** Компьютерная алгебра: Учебник. Нижегородский Государственный Университет им. Н.И. Лобачевского. *http://www.itlab.unn.ru/archive/docs/coaBook.pdf* , 2002. - 102 с.
9. **Курош А.Г.** Теория групп (Издание третье, дополненное). М.: «НАУКА», Главная редакция физико-математической литературы, 1967. - 648 с.
10. **Ноден П., Китте К**. Алгебраическая алгоритмика. Пер. с франц. - М.: Мир, 1999. - 720 с.