




# Новый подход к решению систем уравнений в задачах дискретного логарифмирования



*Выполнила: Савельева А.А.  
Научный руководитель: проф., к.  
т.н. Авдошин С.М.*



# Криптографические системы, основанные на сложности дискретного логарифмирования

- Схема открытого распределения ключей Диффи-Хеллмана
- Схема ЭЦП Эль-Гамала
- ГОСТ Р34.10-2001 (Россия)
- ANSI X9.62/63-2001 (США)

# Алгоритмы дискретного логарифмирования в конечных полях, использующие факторную базу

- Алгоритм Адлемана
  - Алгоритм COS
  - Index-calculus
  - Решето числового поля
- Решение систем линейных уравнений в кольцах вычетов

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

# Постановка задачи

Решить систему  $n$  линейных уравнений с  $m$  неизвестными:

$$a_{1,1}x_1 + \dots + a_{1,m}x_m = b_1$$

$$\boxtimes \quad \boxtimes \quad \boxtimes \quad \boxtimes \quad \boxtimes$$

$$a_{n,1}x_1 + \dots + a_{n,m}x_m = b_n$$

Операции сложения и умножения определены по правилам:

$$\left( \forall c, d \in \mathbf{Z}_p \right) \quad \begin{array}{l} c + d \equiv (c + d) \pmod{p} \\ c \cdot d \equiv (c \cdot d) \pmod{p} \end{array}$$

(здесь  $p$  - некоторое целое положительное число)

# Анализ методов решения систем линейных уравнений в кольцах вычетов

Сведение задачи к :


- решению семейства систем над полями Галуа
- решению системы над кольцом целых чисел
- решению уравнения над кольцом матриц

# Анализ методов решения систем линейных уравнений в кольцах вычетов

Сведение задачи к :

- решению семейства систем над простыми полями
- решению системы над кольцом целых чисел
- решению уравнения над кольцом матриц

# Метод сведения к решению системы над простыми полями: пример


$$\begin{cases} 26x + 3y = 4 \\ 9x + 34y = 1 \end{cases} \pmod{36}$$

Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. - М.: Институт проблем информационной безопасности МГУ, МЦНМО, 2004.

$$36 = 2^2 \cdot 3^2$$

$$\begin{cases} 26x + 3y = 4 \\ 9x + 34y = 1 \end{cases} \pmod{2^2}$$
$$\begin{cases} 2x + 3y = 0 \\ x + 2y = 1 \end{cases} \pmod{4}$$

$$\begin{cases} 26x + 3y = 4 \\ 9x + 34y = 1 \end{cases} \pmod{3^2}$$
$$\begin{cases} 8x + 3y = 4 \\ 7y = 1 \end{cases} \pmod{9}$$



# Метод сведения к решению системы над простыми полями: пример (продолжение)

$$\begin{cases} 2x + 3y = 0 \\ x + 2y = 1 \end{cases} \pmod{4}$$

$$\textcircled{1} \begin{cases} x = x_0 + x_1 \cdot 2 \\ y = y_0 + y_1 \cdot 2 \end{cases} \pmod{4}$$

$$\textcircled{2} \begin{cases} 2x + 3y = 0 \\ x + 2y = 1 \end{cases} \pmod{2} \Rightarrow \begin{cases} 0 \cdot x_0 + 1 \cdot y_0 = 0 \\ 1 \cdot x_0 + 0 \cdot y_0 = 1 \end{cases} \pmod{2}$$

$$\textcircled{2} \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \pmod{2}$$



# Метод сведения к решению системы над простыми полями: пример (продолжение)

$$\begin{cases} 2x + 3y = 0 \\ x + 2y = 1 \end{cases} \pmod{4}$$

$$\textcircled{1} \begin{cases} x = x_0 + x_1 \cdot 2 \\ y = y_0 + y_1 \cdot 2 \end{cases} \pmod{4}$$

$$\textcircled{3} \begin{cases} 2 \cdot x_1 + 2 \cdot y_1 = 2 \\ 2 \cdot x_1 + 4 \cdot y_1 = 0 \end{cases} \pmod{4} \Rightarrow \begin{cases} 1 \cdot x_1 + 1 \cdot y_1 = 1 \\ 1 \cdot x_1 + 0 \cdot y_1 = 0 \end{cases} \pmod{2}$$

$$\textcircled{2} \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \pmod{2}$$

$$\textcircled{3} \begin{pmatrix} x_1 \\ y_1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \pmod{2}$$

# Метод сведения к решению системы над простыми полями: пример (продолжение)

$$\begin{cases} 2x + 3y = 0 \\ x + 2y = 1 \end{cases} \pmod{4}$$

$$\textcircled{1} \begin{cases} x = x_0 + x_1 \cdot 2 \\ y = y_0 + y_1 \cdot 2 \end{cases} \pmod{4} \quad \textcircled{4} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \end{pmatrix} \pmod{4}$$

$$\textcircled{2} \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \pmod{2} \quad \textcircled{3} \begin{pmatrix} x_1 \\ y_1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \pmod{2}$$

# Метод сведения к решению системы над простыми полями: пример (продолжение)

$$\begin{cases} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \end{pmatrix} \pmod{4} \\ \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 8 \\ 4 \end{pmatrix} \pmod{9} \end{cases}$$

По Китайской теореме об остатках:

$$\begin{cases} x = 17 \\ y = 22 \end{cases} \pmod{36}$$



# Недостатки метода сведения к решению семейства систем над простыми полями

- Решение не одной, а **нескольких** систем
- Факторизация числа  $p$ : **открытая проблема** современной теории чисел (не существует алгоритма с полиномиальной сложностью)

# Анализ методов решения систем линейных уравнений в кольцах вычетов

Сведение задачи к :

- решению семейства систем над простыми полями
- **решению системы над кольцом целых чисел**
- решению уравнения над кольцом матриц

# Метод сведения к решению системы над кольцом целых чисел (1): пример

• Сведение:

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

• Общее решение:

Ноден П., Китте К. Алгебраическая алгоритмика. Пер. с франц. - М.: Мир, 1999.

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

**экспоненциальный рост коэффициентов**

# Метод сведения к решению системы над кольцом целых чисел (2): модификации

Способы избежать экспоненциального роста коэффициентов:

- Использование диагональной формы Смита
  - Модификация метода Гаусса
- Полиномиальный  
рост  
коэффициентов

Кузнецов М.И., Бурланков Д.Е., Чирков А.Ю., Яковлев В.А. Компьютерная алгебра: Учебник. - Нижегородский Государственный Университет им. Н.И. Лобачевского. – 2002.

Недостаток:

- Асимптотическая временная и емкостная сложность значительно больше сложности метода Жордана решения систем в полях Галуа



# Анализ методов решения систем линейных уравнений в кольцах вычетов

Сведение задачи к :

- решению семейства систем над простыми полями
- решению системы над кольцом целых чисел
- **решению уравнения над кольцом матриц**

# Метод сведения к уравнению над кольцом матриц

$$Ax=b \quad \longrightarrow \quad x=A^{-1}b$$

Глухов М.М., Елизаров В.П.,  
Нечаев А.А. Алгебра (в 2-х т). Т. I  
- М.: Гелиос АРВ, 2003

Елизаров В.П. Успехи мат.  
наук. – 1993. Т. 48, вып. 2.  
с. 181-182.

## Эффективный алгоритм вычисления обратной матрицы

?

# Предложенный метод

- В основе:
  - Расширенный алгоритм Евклида
  - Схема Жордана
- Применим для:
  - кольцо вычетов
  - полей Галуа
- Эффективность:
  - По временной и емкостной сложности эквивалентен классическим алгоритмам Жордана и Гаусса решения систем в полях Галуа

# Расширенный алгоритм Евклида

- Вход:  $a, b \in \mathbf{Z}_+$
- Выход:  $d, x, y, r, s$  такие, что  $\begin{cases} \text{НОД}(a, b) = d \\ 0 = a \cdot r + b \cdot s \end{cases}$

**АЛГ** *Евклид*( $a, b$ )

$$\begin{pmatrix} d & x & y \\ n & r & s \end{pmatrix} \leftarrow \begin{pmatrix} a & 1 & 0 \\ b & 0 & 1 \end{pmatrix}$$

**ПОКА**  $n \geq 0$  **ЦИКЛ**

$$c \leftarrow \lfloor d / n \rfloor$$

$$\begin{pmatrix} d & x & y \\ n & r & s \end{pmatrix} \leftarrow \begin{pmatrix} 0 & 1 \\ 1 & -c \end{pmatrix} \times \begin{pmatrix} d & x & y \\ n & r & s \end{pmatrix}$$

**К.Ц.**

**К.АЛГ.**

# Схема Жордана

$$\left( \begin{array}{ccc|ccc|c} a_{11} & \boxtimes & \boxtimes & a_{1n} & a_{1,n+1} & \boxtimes & a_{1,m} & b_1 \\ \boxtimes & \boxtimes & & \boxtimes & \boxtimes & & \boxtimes & \boxtimes \\ \boxtimes & & \boxtimes & \boxtimes & \boxtimes & & \boxtimes & \boxtimes \\ a_{n1} & \boxtimes & \boxtimes & a_{nn} & a_{n,n+1} & \boxtimes & a_{n,m} & b_n \end{array} \right)$$



$$\left( \begin{array}{ccc|ccc|c} 1 & 0 & \boxtimes & 0 & a'_{1,i_{n+1}} & \boxtimes & a'_{1,i_m} & b'_1 \\ 0 & \boxtimes & & \boxtimes & \boxtimes & & \boxtimes & \boxtimes \\ \boxtimes & & \boxtimes & 0 & \boxtimes & & \boxtimes & \boxtimes \\ 0 & \boxtimes & 0 & 1 & a'_{n,i_{n+1}} & \boxtimes & a'_{n,i_m} & b'_n \end{array} \right)$$

# Матрицы над кольцом

**Опр.1** Множество всех матриц размером  $m \times n$  с элементами из кольца  $R$  будем обозначать через  $R_{m,n}$

**Элементарными преобразованиями строк** матрицы  $A \in R_{m,n}$  называют:

- умножение любой ее строки на обратимый элемент кольца  $R$ ;
- прибавление к любой ее строке другой строки, умноженной на произвольный элемент кольца  $R$ ;
- транспозицию строк.

**Опр.2** Матрица  $B \in R_{m,n}$  называется **строчно эквивалентной матрице**  $A \in R_{m,n}$ , если она может быть получена из  $A$  с помощью конечной последовательности элементарных преобразований строк.

# Применение алгоритма Евклида к матрице

Коэффициенты Безу для  $a=26$ ,  $b=9$  :

$$1 = 26 \cdot (35) + 9 \cdot (3) \quad 0 = 26 \cdot (9) + 9 \cdot (10)$$

$$\begin{array}{l}
 [1] \quad \left( \begin{array}{cc|c} 26 & 3 & 4 \\ 9 & 34 & 1 \end{array} \right) \xrightarrow{[1]-[2] \cdot 2} \left( \begin{array}{cc|c} 8 & 7 & 2 \\ 9 & 34 & 1 \end{array} \right) \xrightarrow{[1] \leftrightarrow [2]} \left( \begin{array}{cc|c} 9 & 34 & 1 \\ 8 & 7 & 2 \end{array} \right) \\
 [2] \quad \left( \begin{array}{cc|c} 9 & 34 & 1 \\ 8 & 7 & 2 \end{array} \right) \xrightarrow{[1]-[2] \cdot 1} \left( \begin{array}{cc|c} 1 & 27 & 35 \\ 8 & 7 & 2 \end{array} \right) \xrightarrow{[1] \leftrightarrow [2]} \left( \begin{array}{cc|c} 8 & 7 & 2 \\ 1 & 27 & 35 \end{array} \right) \\
 [1] \quad \left( \begin{array}{cc|c} 8 & 7 & 2 \\ 1 & 27 & 35 \end{array} \right) \xrightarrow{[1]-[2] \cdot 8} \left( \begin{array}{cc|c} 0 & 7 & 10 \\ 1 & 27 & 35 \end{array} \right) \xrightarrow{[1] \leftrightarrow [2]} \left( \begin{array}{cc|c} 1 & 27 & 35 \\ 0 & 7 & 10 \end{array} \right) \\
 [1] \quad \left( \begin{array}{cc|c} 1 & 27 & 35 \\ 0 & 7 & 10 \end{array} \right) \xrightarrow{[2] \cdot 31} \left( \begin{array}{cc|c} 1 & 27 & 35 \\ 0 & 1 & 22 \end{array} \right) \xrightarrow{[1]-[2] \cdot 27} \left( \begin{array}{cc|c} 1 & 0 & 17 \\ 0 & 1 & 22 \end{array} \right)
 \end{array}$$



# Работа алгоритма

- Решение системы: 
$$\begin{cases} 26x + 3y = 4 \\ 9x + 34y = 1 \end{cases} \pmod{36}$$

$$\begin{array}{l} [1] \\ [2] \end{array} \left( \begin{array}{cc|c} 26 & 3 & 4 \\ 9 & 34 & 1 \end{array} \right) \xrightarrow{\begin{array}{l} [1]'=[1]\cdot 35+[2]\cdot 3 \\ [2]'=[1]\cdot 9+[2]\cdot 10 \end{array}} \left( \begin{array}{cc|c} 1 & 27 & 35 \\ 0 & 7 & 10 \end{array} \right) \xrightarrow{\begin{array}{l} [1]'=[1]+[2]\cdot 27 \\ [2]'=[2]\cdot 31 \end{array}} \left( \begin{array}{cc|c} 1 & 0 & 17 \\ 0 & 1 & 22 \end{array} \right)$$

- Вычисление обратной матрицы:

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

$$\begin{array}{l} [1] \\ [2] \end{array} \left( \begin{array}{cc|cc} 1 & 27 & 35 & 3 \\ 0 & 7 & 9 & 10 \end{array} \right) \xrightarrow{\begin{array}{l} [1]'=[1]+[2]\cdot 27 \\ [2]'=[2]\cdot 31 \end{array}} \left( \begin{array}{cc|cc} 1 & 0 & 26 & 21 \\ 0 & 1 & 27 & 22 \end{array} \right)$$

# Алгоритм

- **Вход:**  $A = (a_{ij})_{n \times m}$  {рациональная матрица},  $a_{ij} \in \mathbf{Z}_p$
- **Выход:**  $A$  {преобразованная матрица}

**АЛГ Жордан**( $A, n, m, p$ )

**ДЛЯ**  $i=1$  **ДО**  $n$  **ЦИКЛ**

{обнуляем эл-ты  $i$ -го столбца ниже  $i$ -й строки}

**ДЛЯ**  $j=i+1$  **ДО**  $n$  **ЦИКЛ**

**ВЫЧИСЛИТЬ**  $x', y', r', s' : \left\{ \begin{array}{l} \text{НОД}(a_{ii}, a_{ji}) = a_{ii} \cdot x' + a_{ji} \cdot y' \\ 0 = a_{ii} \cdot r' + a_{ji} \cdot s' \end{array} \right\}$

$$\begin{pmatrix} A(i, *) \\ A(j, *) \end{pmatrix} \leftarrow \begin{pmatrix} x' & y' \\ r' & s' \end{pmatrix} \times \begin{pmatrix} A(i, *) \\ A(j, *) \end{pmatrix}$$

**К.Ц.** {для  $j$ }

# Алгоритм (продолжение)



**ЕСЛИ**  $\text{НОД}(a_{ii}, p) > 1$

**ТО** выйти из алгоритма *{матрица вырождена}*

**ИНАЧЕ**

*{обнуляем элементы  $i$ -го столбца выше  $i$ -й строки}*

$$A(i, *) := A(i, *) \cdot a_{i,i}^{-1}$$

$$A(j, *) \leftarrow A(j, *) - A(i, *) \cdot a_{ji}, \quad j = \overline{1, i-1}$$

**К.Е.**

**ВЕРНУТЬ(A)**

**К.АЛГ.**

# Временная сложность алгоритмов

<p>Метод сведения к полям Гауа (при <math>p = \prod_{k=1}^t q_k^{\alpha_k}</math>)</p>	<p>Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. - М.: Институт проблем информационной безопасности МГУ, МЦНМО, 2004</p>
<p>Метод сведения к диофантовым уравнениям (с построением матрицы Смита)</p>	<p>Кузнецов М.И., Бурланков Д.Е., Чирков А.Ю., Яковлев В. А. Компьютерная алгебра: Учебник. - Нижегородский Государственный Университет им. Н.И. Лобачевского. – 2002.</p>
<p>Метод сведения к уравнению над кольцом матриц</p>	<p>Глухов М.М., Елизаров В.П., Нечаев А.А. Алгебра (в 2-х т). Т. I - М.: Гелиос АРВ, 2003 Елизаров В.П. Успехи мат. наук.–1993.Т. 48, вып. 2.</p>
<p>Метод, предложенный в данной работе</p>	<p>Авдошин С.М., Савельева А.А. Свид. Об официальной регистрации программы для ЭВМ № 2005612258: «Программа решения систем линейных уравнений в кольцах вычетов». Зарегистрировано в Реестре программ для ЭВМ 02.09.2005</p>

# Временная сложность алгоритмов

<p>Метод сведения к полям Гауа (при <math>p = \prod_{k=1}^t q_k^{\alpha_k}</math>)</p>	$O\left(n \cdot (n \cdot m \cdot \sum_{k=1}^t \alpha_k + \log p) + \sqrt{\ln p \ln \ln p} \cdot e^{\sqrt{\ln p \ln \ln p}}\right)$
<p>Метод сведения к диофантовым уравнениям (с построением матрицы Смита)</p>	<p>Кузнецов М.И., Бурланков Д.Е., Чирков А.Ю., Яковлев В. А. Компьютерная алгебра: Учебник. - Нижегородский Государственный Университет им. Н.И. Лобачевского. – 2002.</p>
<p>Метод сведения к уравнению над кольцом матриц</p>	<p>Глухов М.М., Елизаров В.П., Нечаев А.А. Алгебра (в 2-х т). Т. I - М.: Гелиос АРВ, 2003 Елизаров В.П. Успехи мат. наук.–1993.Т. 48, вып. 2.</p>
<p>Метод, предложенный в данной работе</p>	<p>Авдошин С.М., Савельева А.А. Свид. Об официальной регистрации программы для ЭВМ № 2005612258: «Программа решения систем линейных уравнений в кольцах вычетов». Зарегистрировано в Реестре программ для ЭВМ 02.09.2005</p>

# Временная сложность алгоритмов

<p>Метод сведения к полям Гауа (при <math>p = \prod_{k=1}^t q_k^{\alpha_k}</math>)</p>	$O\left(n \cdot (n \cdot m \cdot \sum_{k=1}^t \alpha_k + \log p) + \sqrt{\ln p \ln \ln p} \cdot e^{\sqrt{\ln p \ln \ln p}}\right)$
<p>Метод сведения к диофантовым уравнениям (с построением матрицы Смита)</p>	$O(n^2 m^2 \log p)$
<p>Метод сведения к уравнению над кольцом матриц</p>	<p>Глухов М.М., Елизаров В.П., Нечаев А.А. Алгебра (в 2-х т). Т. I - М.: Гелиос АРВ, 2003 Елизаров В.П. Успехи мат. наук.–1993.Т. 48, вып. 2.</p>
<p>Метод, предложенный в данной работе</p>	<p>Авдошин С.М., Савельева А.А. Свид. Об официальной регистрации программы для ЭВМ № 2005612258: «Программа решения систем линейных уравнений в кольцах вычетов». Зарегистрировано в Реестре программ для ЭВМ 02.09.2005</p>



# Временная сложность алгоритмов

<p>Метод сведения к полям Гауа (при <math>p = \prod_{k=1}^t q_k^{\alpha_k}</math>)</p>	$O\left(n \cdot (n \cdot m \cdot \sum_{k=1}^t \alpha_k + \log p) + \sqrt{\ln p \ln \ln p} \cdot e^{\sqrt{\ln p \ln \ln p}}\right)$
<p>Метод сведения к диофантовым уравнениям (с построением матрицы Смита)</p>	$O(n^2 m^2 \log p)$
<p>Метод сведения к уравнению над кольцом матриц</p>	$O(n^n)$
<p>Метод, предложенный в данной работе</p>	<p>Авдошин С.М., Савельева А.А. Свид. Об официальной регистрации программы для ЭВМ № 2005612258: «Программа решения систем линейных уравнений в кольцах вычетов». Зарегистрировано в Реестре программ для ЭВМ 02.09.2005</p>



# Временная сложность алгоритмов

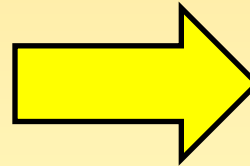
<p>Метод сведения к полям Гауа (при <math>p = \prod_{k=1}^t q_k^{\alpha_k}</math>)</p>	$O\left(n \cdot (n \cdot m \cdot \sum_{k=1}^t \alpha_k + \log p) + \sqrt{\ln p \ln \ln p} \cdot e^{\sqrt{\ln p \ln \ln p}}\right)$
<p>Метод сведения к диофантовым уравнениям (с построением матрицы Смита)</p>	$O(n^2 m^2 \log p)$
<p>Метод сведения к уравнению над кольцом матриц</p>	$O(n^n)$
<p>Метод, предложенный в данной работе</p>	$O(n \cdot (nm + \log p))$

# Решение систем, возникающих при дискретном логарифмировании

- **Свойства:**

- Большой размер (миллионы уравнений с миллионами неизвестных)
- Разреженные матрицы

**Поля:**  
структурированное  
гауссово исключение



**Кольца:**  
модифицированный  
алгоритм  
структурированного  
гауссова исключения

# Заключение

## Результаты, полученные в данной работе:

- Проведен анализ известных методов решения систем линейных уравнений над кольцом вычетов
- Разработан алгоритм, эквивалентный по сложности методам Жордана и Гаусса решения систем линейных уравнений над полями Галуа
- Программа, реализующая разработанный алгоритм, зарегистрирована Федеральной службой по интеллектуальной собственности, патентам и товарным знакам (Роспатент)
- Результаты исследований опубликованы в журнале «Информационные технологии» (№2, 2006)

# Направление дальнейшей работы

- Теоретическое и экспериментальное исследование влияния полученного метода на временную сложность алгоритмов дискретного логарифмирования, использующие факторную базу:
  - Алгоритм Адлемана
  - Index-calculus
  - Алгоритм COS
  - Решето числового поля

# Кольца вычетов

Операции сложения и умножения определяют **кольцо вычетов по модулю  $p$**  ( $\mathbf{Z}_p$ ). Оно является коммутативным кольцом с единицей.

**Опр.1 Делителем нуля** в произвольном кольце  $R$  называется любой его элемент  $a \neq 0$ , для которого в  $R$  существует элемент  $b \neq 0$ , удовлетворяющий условию  $a \cdot b = 0$  или  $b \cdot a = 0$

**Опр.2 Обратимым элементом** в произвольном кольце  $R$  называется любой его элемент  $a \neq 0$ , для которого в  $R$  существует обратный элемент  $a^{-1}$ , удовлетворяющий условию  $a \cdot a^{-1} = 1$  или  $a^{-1} \cdot a = 1$

# Обратный элемент

Элемент  $x^{-1} \in \mathbf{Z}_p$  называется **обратным** к  $x \in \mathbf{Z}_p$ , если

$$x \cdot x^{-1} = x^{-1} \cdot x \equiv 1 \pmod{p}.$$

Для нахождения обратного элемента нужно решить линейное диофантово уравнение:

$$u \cdot x + v \cdot p = 1$$

Уравнение разрешимо относительно  $u$  и  $v$  тогда и только тогда, когда  $\text{НОД}(x, p) = 1$ ; в этом случае  $x^{-1} = u$ . Для вычисления  $u$  и  $v$  (**коэффициентов Безу**) используется **расширенный алгоритм Евклида**.

# Пример решения системы в поле Галуа порядка 37

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

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

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



# Пример решения системы в кольце вычетов по модулю 36

$$26 \cdot 18 \equiv 0 \pmod{36}$$

$$3 \cdot 12 \equiv 0 \pmod{36}$$

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

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

$$9 \cdot 4 \equiv 0 \pmod{36}$$

$$34 \cdot 18 \equiv 0 \pmod{36}$$

Все коэффициенты системы являются делителями нуля, т.е. необратимы. Однако решение существует и единственно:

$$\begin{cases} x = 17 \\ y = 22 \end{cases}$$