|  |
| --- |
| МИНОБРНАУКИ РОССИИ |
| Федеральное государственное бюджетное образовательное учреждение  высшего образования  **«МИРЭА – Российский технологический университет»**  **РТУ МИРЭА** |

|  |  |  |  |
| --- | --- | --- | --- |
| **ЛЕКЦИЯ № 6** | | | |
| по дисциплине: | | **Б2.В,ДВ.3.1 «Криптографические методы защиты информации»** | |
|  | | (шифр и наименование учебной дисциплины) | |
| по теме: | Матрицы и сравнения. | | |
|  | (наименование темы лекции) | | |
|  | | |
|  | | |  |
| Институт Кибербезопасности и цифровых технологий.  Кафедра КБ-8 Информационное противоборство,  МИРЭА – 2020 г. | | | |

Тема лекции: Матрицы. Действия над матрицами.Детерминант матрицы.Инверсия. Линейные уравнения с одним неизвестным содержащие сравнения.

Учебные и воспитательные цели:

1. Матрицы. Действия над матрицами

2.Детерминант матрицы.Инверсия.

3.Решение системы линейных сравнений с одним неизвестным.ШифрХилла.

**Время:** 2 часа (90 мин.).

Литература:

а) Основная:

1. Рябко Б.Я.,Фионов А.Н. Криптография в современном мире.-М.: Горячая линия-Телеком, 2018.-300с.:ил.

2. Горбенко А.О., Основы информационной безопасности: введение в профессию.Учебное пособие, СПб: ИЦ «Интермедия», 2016.‒ 224 с.

3. Бутакова Н.Г., Федоров Н.В. Криптографические методы защиты информации. Учебное пособие, СПб: ИЦ «Интермедия», 2016. ‒ 312 с.

4.Хорев А.А., Защита информации от утечки по техническим каналам. Учебник. СПб: ИЦ «Интермедия», 2016. 920 с.

б) Дополнительная литература:

1. Зайцев А.П. и др. Технические средства и методы защиты информации. Уч. пособие. М.: Горячая линия – Телеком. 2009. – 615 с.

2. Романец Ю.В. и др. Защита информации в компьютерных системах и сетях. М.: Радио и связь. 1999. – 376 с.

3. Лозовецкий В.В. Информационная безопасность. М.: Изд. ИУИ. 2011. – 169 с.

Учебно-материальное обеспечение:

Наглядные пособия.

Технические средства обучения: проектор.

Приложения: рисунки, таблицы, слайды.

ПЛАН ЛЕКЦИИ:

**Введение** – до 5 мин.

**Основная часть** (учебные вопросы) – до 80 мин.

1. Матрицы. Действия над матрицами-25 мин.

2.Детерминант матрицы.Инверсия -25 мин.

3.Решение системы линейных сравнений с одним неизвестным.-30 мин.

Заключение – до 5 мин.

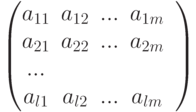
Введение – до 5 мин.

**5.1. Матрицы**

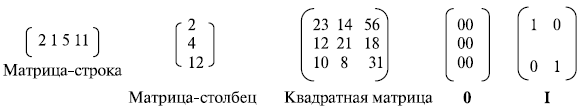
В криптографии мы должны обрабатывать матрицы. Хотя эта тема принадлежит специальному разделу алгебры, который называется линейной алгеброй, необходим краткий обзор матриц для подготовки к изучению криптографии. Читатели, знакомые с этими вопросами, могут пропустить часть или весь этот раздел. Раздел начинается с некоторых определений и примеров использования матрицы в модульной арифметике.

**Определения**

**Матрица** — *прямоугольный массив*, содержащий l x m элементов, в которых l — число строк, m — число столбцов. Матрица обычно обозначается заглавной буквой, такой, как A. Элемент aij расположен в i -той строке и j -том столбце. Хотя элементы матрицы могут быть любым множеством чисел, мы обсуждаем только матрицы с элементами в Z. Пример матрицы с m столбцами и l строками



Если матрица имеет только одну строку ( l = 1 ), она называется **матрицей-строкой** ; если она имеет только один столбец ( m = 1 ), то называется **матрицей-столбцом**. Матрица называется квадратной, если число строк равно числу столбцов ( l = m ) и содержит элементы a11, a22, ……, amm. Матрица обозначается 0, если все строки и все столбцы содержат нули. **Единичная матрица** обозначается I, если она квадратная и содержит все единицы на главной диагонали и все нули на других местах. [Рисунок 6.2](#image.3.2) показывает некоторые примеры матриц с элементами из Z.



**Рис. 6.2.**Примеры матриц

**Операции и уравнения**

В линейной алгебре для матриц определены одно уравнение (равенство) и четыре операции (сложение, вычитание, умножение и *скалярное умножение*).

**Равенство**

Две матрицы равны, если они имеют одинаковое число строк и столбцов и соответствующие элементы равны. **Другими словами**, A = B, если мы имеем aij = bij для всех i и j.

**Сложение и вычитание**

**Операция сложения двух матриц может применяться, если матрицы имеют одинаковое число столбцов и строк. Сложение записывают как C =A + B. В этом случае полученная в результате матрица C имеет тот же самый номер строк и столбцов, как A или B. Каждый элемент C — сумма двух соответствующих элементов A и B: aij + bij.**

**Операция вычитания производится аналогично сложению, за исключением того, что каждый элемент B вычитается из соответствующего элемента A: dij= aij – bij.**

**Пример 5.1**

Ниже показан пример сложения и вычитания.



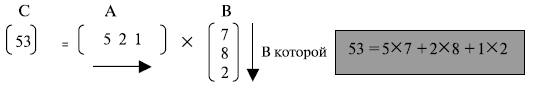
**Умножение**

Две матрицы различного размера могут быть перемножены, если число столбцов первой матрицы совпадает с числом строк второй матрицы. Если A — матрица размера l x m, а матрица B размера m x p, то произведением будет матрица C размером l x p. Если элемент матрицы A обозначить aij, а каждый элемент матрицы B обозначить bjk, то элемент матрицы C — cik — вычисляется следующим образом:



**Пример 6.2**

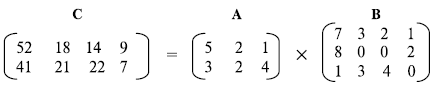
[Рисунок 6.3](#image.3.3) показывает произведение матрицы-строки (  ) на матрицу-столбец (  ). В результате получаем матрицу размером .



**Рис. 6.3.**Умножение матрицы-строки на матрицу-столбец

**Пример 6.4**

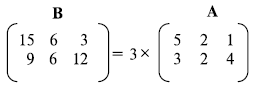
[Рисунок 6.4](#image.3.4) показывает произведение матрицы  на матрицу . В результате получаем матрицу 



**Рис. 6.4.**Умножение матрицы 2 x 3 на матрицу 3 x 4.

**Скалярное умножение**

Мы можем также умножить матрицу на число (называемое **скаляр** ). Если A — матрица  и x — скаляр, то C = xA — матрица , в которой .



**Рис. 6.5.**Скалярное умножение

**Пример 6.6**

Рисунок 6.5 показывает пример *скалярного умножения*.

**2.Детерминант матрицы.Инверсия -25 мин.**

**Детерминант** — квадратная матрица A размера , обозначаемая как det (A) — скалярное вычисление рекурсивно, как это показано ниже:

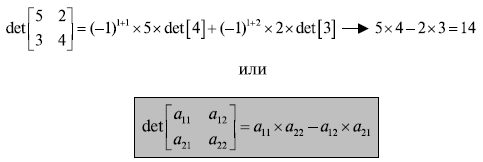
* 
* 

где Aij получается из A удалением i -той строки j -того столбца.

**Детерминант определяется только для квадратной матрицы**.

**Пример 6.5**

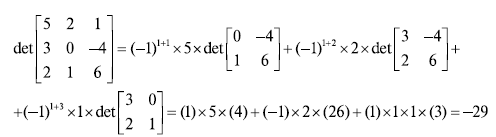
[Рисунок 6.6](#image.3.6) показывает, как можно вычислить *детерминант* матрицы , базируясь на детерминанте матрицы  и используя приведенное выше *рекурсивное определение*. Пример доказывает, что когда m 1 или 2, это позволяет найти *детерминант* матрицы достаточно просто.



**Рис. 6.6.**Вычисление детерминанта матрицы 2 x 2

**Пример 6.6**

[Рисунок 6.7](#image.3.7) показывает вычисление детерминанта матрицы .



**Рис. 6.7.**Вычисление детераминаната матрицы 3 x 3

**Инверсии**

Матрицы имеют аддитивные и мультипликативные *инверсии*.

**Аддитивная инверсия**

Аддитивная *инверсия* матрицыA — это другая матрица B, такая, что A + B = 0. Другими словами, мы имеем элементы bij = –aij для всех значений i и j. Обычно аддитивная *инверсия* A обозначается как (-A).

**Мультипликативная инверсия**

Мультипликативная *инверсия* определена только для квадратных матриц. Мультипликативная *инверсия* квадратной матрицы A — квадратная матрица B, такая, что . Обычно мультипликативная *инверсия* обозначается как A-1. Мультипликативная *инверсия* существует только, если det (A) имеет мультипликативную *инверсию* в соответствующем инверсном множестве. Если целое число не имеет мультипликативной *инверсии* в Z, то не существует мультипликативной *инверсии* матрицы в Z. Однако матрицы с реальными элементами имеют *инверсии*, только если .

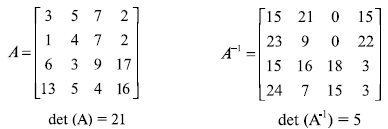
**Мультипликативные инверсии определены только для квадратных матриц**.

**Матрицы вычетов**

Криптография использует матрицы вычетов: матрицы могут содержать все элементы из Zn. Все операции на матрицах вычетов выполняются так же, как и на матрицах целых чисел, за исключением того, что операции производятся в модульной арифметике. Есть одно интересное свойство: **матрица вычетов имеет мультипликативную*****инверсию*, если*****детерминант* матрицы имеет мультипликативную*****инверсию* в Zn. Другими словами, матрица вычета имеет мультипликативную*****инверсию*, если НОД (det (A), n) = 1.**

**Пример 6.7**

[Рисунок 6.8](#image.3.8) показывает матрицу вычетов в Zn и его мультипликативной *инверсии* A-1. Возьмем *детерминант* det (A) = 21, который имеет мультипликативную *инверсию* 5 в Z26. Обратите внимание, что когда мы умножаем эти две матрицы, то результат — *единичная матрица* мультипликативная матрица, в Z26.



**Рис. 6.8.**Матрица вычетов и мультипликативная инверсия

**Сравнение**

**Две матрицы, сравнимые по модулю n, записываются как , если они имеют одинаковое число строк и столбцов и все соответствующие элементы — сравнимые по модулю n. Другими словами, , если  для всех i и j.**

**3. Решение системы линейных сравнений . -30 мин.**

Пусть есть система сравнений

2x+3y=1 (mod26)

7x+8y=2(mod26)

Вычислить x,y.

Запишем данную систему в матричном видеА\*X=Cmod 26,тогда X=A(^(-1))Cmod26.

Для данной системы матрицы А,Х, С будут иметь вид:

2 3 x 1

A= 7 8 X= y C= 2

Вычислим определитель матрицыА

detA= 2 3 = 16-21= -5

7 8

2 7

Построим транспонированную матрицу Ат= 3 8

8 -3

Вычислим матрицу дополнений Атд=-7 2

Тогда обратная матрица может быть вычислена путём деления матрицы Атд на детерминант, то есть

А(^(-1))=Атд\*(-1\5)

Умножив (-1) на числа матрицы Атд получим

-8 3

А(^(-1))=1\5 \* 7 -2 .

Вычислим 5(^(-1)) по mod26 с помощью функции Эйлера

5(^(-1)) по mod26 = 5(^11)) mod26= 21 mod 26.

18 3 378 63 14 11

Тогда А(^(-1))= 21 \* 7 24 = 147 504 = 17 10

Проверим правильность вычисления обратной матрицы

2 3 14 11 1 0

А\*A(^(-1))= 7 8 17 10 = 0 1

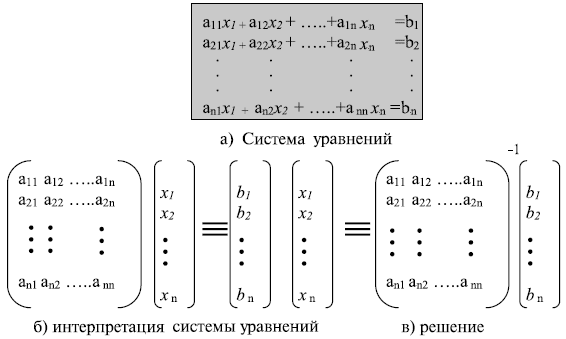
Вычислим вектор Х = А(^(-1))\*C

14 11\* 1 36 10

Получим X= 17 10 2 = 37 (mod26) = 11

То есть х=10 mod 26 y= 11 mod26.

Таким образом, система сравнений n-ого порядка может быть решена, используя подход предложенный выше.



**Рис. 6.9.**Система линейных уравнений

**Пример 6.11**

Решение системы следующих трех уравнений то есть системы 3-го порядка:

**3x + 5y + 7z = 3 (mod 16)**

**x + 4y + 13z = 5 (mod 16)**

**2x + 7y + 3z = 4 (mod 16)**

**Решение**

Здесь x, y и z играют роли x1, x2, и x3. Вычисляем детерминант матрицы, так как он не равен нулю, то матрица, сформированная из коэффициентов уравнений, — обратима. Мы находим мультипликативную *инверсию* матрицы и умножаем ее на матрицу столбца, сформированную из 3, 5 и 4. Результат — ,  и . Мы можем проверить ответ, подставляя эти значения в уравнения.

****

**5.4. Итоги**

* Множество целых чисел, обозначаемое Z, содержит все целые числа от отрицательной бесконечности до положительной бесконечности. Для целых чисел определены три общих *бинарных операции* — сложение, вычитание и умножение. Деление не удовлетворяет определению бинарности, потому что требует два выхода вместо одного.
* В арифметике целых чисел, если мы делим a на n, мы можем получить q и r. Отношение между этими четырьмя целыми числами можно показать как . Мы говорим a|n, если . В этой лекции мы рассмотрели четыре свойства теории *делимости*.
* Два положительных целых числа могут иметь больше чем один общий делитель. Но мы обычно интересуемся наибольшим общим делителем. *Алгоритм Евклида* дает эффективный и систематический алгоритм вычисления наибольшего общего делителя двух целых чисел.
* Расширенный алгоритм Эвклида может вычислить НОД (a, b) и вычислить значение s и t, которые удовлетворяют уравнению as + bt = НОД (a, b). Линейное диофантово уравнение двух переменных: ax + by = c. Оно имеет частное и общие решения.
* В модульной арифметике мы интересуемся только остатками; мы хотим знать значение r, когда мы делим a на n. Мы используем новый оператор, названный модулем (mod), такой, что a mod n = r. Здесь n называется модулем, а r называется *вычетом*.
* Результат операции по модулю n — всегда целое число от 0 и до n-1. Мы можем сказать, что операция по модулю n создает набор, который в модульной арифметике называется множеством наименьших вычетов по модулю n, или Zn.
* Отображение из Z в Zn не совпадают один в один. Определенные элементы Z могут быть отображены в элемент Zn. В модульной арифметике все целые числа в Z, отображаемые в Zn, называются сравнениями по модулю. Для обозначения этой операции применяется оператор сравнения (  ).
* Система вычетов [a] — множество целых чисел, сравнимых по модулю n. Это множество всех целых чисел x = a (mod n).
* Три *бинарных операции* (сложение, вычитание и умножение), определенные для множества Z, могут быть также определены для множества Zn. При необходимости результат может быть отражен в Zn при помощи операции mod.
* В этой лекции для модульных операторов были определены несколько свойств.
* В Zn два числа a и b — аддитивные *инверсии* по отношению друг к другу, если . Они — мультипликативные *инверсии* по отношению друг к другу, если . Целое число a имеет мультипликативную *инверсию* в Zn тогда и только тогда, когда НОД (n, a) = 1 ( a и n — взаимно простые числа).
* Расширенный *алгоритм Евклида* находит мультипликативные *инверсии* b в Zn, когда даны n и b и НОД (n, b) = 1. Мультипликативная *инверсия* b — это значение t при соответствующем отображении в Zn.
* Матрица — *прямоугольный массив* . элементы, где l является номером строки, а m — номер столбца. Мы обозначаем матрицу заглавной буквой и жирным шрифтом, например, A. Элемент aij расположен в i -той строке и j -том столбце.
* Две матрицы равны, если они имеют одинаковое число строк и столбцов и соответствующие элементы равны.
* Сложение и вычитание можно делать только для матриц равного размера. Мы можем умножить друг на друга две матрицы различных размеров, если число столбцов первой матрицы совпадает с числом строк второй матрицы. В матрицах вычетов все элементы берутся из Zn.
* Все операции на матрицах вычетов проводятся в модульной арифметике.
* Матрица вычета имеет *инверсию*, если *детерминант* матрицы имеет *инверсию*.
* Уравнение  не может иметь решения или ограниченное число решений. Если НОД (a,n)|b, то имеется ограниченное число решений.
* Система *линейных уравнений* с тем же самым модулем может быть решена, если матрица, сформированная из коэффициентов уравнений, имеет *инверсию*.

Описание шифра Хилла[

Шифр Хилла является [полиграммным шифром](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80_%D0%BF%D0%BE%D0%B4%D1%81%D1%82%D0%B0%D0%BD%D0%BE%D0%B2%D0%BA%D0%B8#%D0%9F%D0%BE%D0%BB%D0%B8%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%BD%D1%8B%D0%B5_%D1%88%D0%B8%D1%84%D1%80%D1%8B), который может использовать большие блоки с помощью линейной алгебры. Каждой букве алфавита сопоставляется число по модулю 26. Для латинского алфавита часто используется простейшая схема: A = 0, B = 1, …, Z = 25, но это не является существенным свойством шифра. Блок из *n* букв рассматривается как *n*-мерный вектор и умножается по модулю 26 на матрицу размера *n* × *n*. Если в качестве основания модуля используется число больше чем 26, то можно использовать другую числовую схему для сопоставления буквам чисел и добавить пробелы и знаки пунктуации[[5]](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80_%D0%A5%D0%B8%D0%BB%D0%BB%D0%B0#cite_note-:2-5). Элементы матрицы являются ключом. Матрица должна быть обратима в Zn-26чтобы была возможна операция расшифрования.

Для *n* = 3 система может быть описана так:

C1= K11\*P1+K12\*P2 +K13\*P3 ( mod 26)

C2= K21\*P1+K22\*P2 + K23\*P3 ( mod 26)

C3=K31\*P1+K32\*P2 + K33\*P3 ( mod 26)

Или в векторной форме

С1 k11 k12 k13 p1

С2 = k21 k22 k23 \* p2 (mod 26)

С3 k31 k32 k33 p3

где P и C — векторы-столбцы высоты 3, представляющие открытый и зашифрованный текст соответственно, K— матрица 3 × 3, представляющая ключ шифрования. Операции выполняются по модулю 26.

То есть С=K\*Pmod 26

Для того, чтобы расшифровать сообщение, требуется получить обратную матрицу ключа K^{-1}. Существуют стандартные методы вычисления обратных матриц,но не все матрицы имеют обратную.Матрица будет иметь обратную в том и только в том случае, когда её детерминант не равен нулю и не имеет общих делителей с основанием модуля[[](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80_%D0%A5%D0%B8%D0%BB%D0%BB%D0%B0#cite_note-:3-8). Если детерминант матрицы равен нулю или имеет общие делители с основанием модуля, то такая матрица не может использоваться в шифре Хилла, и должна быть выбрана другая матрица (в противном случае шифротекст будет невозможно расшифровать). Тем не менее, матрицы, которые удовлетворяют вышеприведенным условиям, существуют в изобилии.

В общем случае, алгоритм шифрования может быть выражен в следующем виде

**Шифрование:C=E(K,P)=K\*Pmod 26**

**РасшифрованиеP=D(K,C)=K^{-1}\*C{mod {26}}=K^{-1}\*K\*Pmod {26}}=P**.

Пример[В следующем примере[[7]](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80_%D0%A5%D0%B8%D0%BB%D0%BB%D0%B0#cite_note-:4-7) используются латинские буквы от A до Z, соответствующие им численные значения приведены в таблице.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **A** | **B** | **C** | **D** | **E** | **F** | **G** | **H** | **I** | **J** | **K** | **L** | **M** | **N** | **O** | **P** | **Q** | **R** | **S** | **T** | **U** | **V** | **W** | **X** | **Y** | **Z** |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

**Шифрование**

Рассмотрим сообщение «ACT» и представленный ниже ключ (GYBNQKURP- в буквенном виде): 6 24 1

K= 13 16 10

20 17 15

Вычислить определитель матрицы- 10 мин

Данная матрица обратима, так как её детерминант не равен нулю и не имеет общих делителей с основанием модуля. Опасность того, что детерминант матрицы ключа будет иметь общие делители с основанием модуля, может быть устранена путём выбора простого числа в качестве основания модуля. Например, в более удобном варианте шифра Хилла в алфавит добавляют 3 дополнительных символа **(пробел, точка и знак вопроса)**, чтобы увеличить основание модуля до 29[[5]](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80_%D0%A5%D0%B8%D0%BB%D0%BB%D0%B0#cite_note-:2-5).

Так как букве «A» соответствует число 0, «C» — 2, «T» — 19, то сообщение — это вектор

P1= 0

2

19

Тогда зашифрованный вектор С1 будет

6 24 1 0 15

С1=K\*P1 mod 26= 13 16 10 \* 2 mod26 = 14

20 17 15 19 7

Вектор соответствует зашифрованному тексту «POH».

**Теперь предположим**, что наше сообщение было «CAT»:тогдасообщение — это вектор 2

P2= 0

19

Выполняя операции аналогичные в ранее рассмотренном примере получим :

6 24 1 2 5 F

С2=K\*P2 mod 26= 13 16 10 \* 0 mod26 = 8 I

20 17 15 19 13 N

Этот вектор соответствует зашифрованному тексту «FIN». Видно, что каждая буква шифротекста сменилась. Шифр Хилла достиг [диффузии](https://ru.wikipedia.org/w/index.php?title=%D0%9A%D0%BE%D0%BD%D1%84%D1%83%D0%B7%D0%B8%D1%8F_%D0%B8_%D0%B4%D0%B8%D1%84%D1%84%D1%83%D0%B7%D0%B8%D1%8F&action=edit&redlink=1) по [Шеннону](https://ru.wikipedia.org/wiki/%D0%A8%D0%B5%D0%BD%D0%BD%D0%BE%D0%BD,_%D0%9A%D0%BB%D0%BE%D0%B4), и *n*-размерный шифр Хилла может достигать диффузии *n* символов за раз.

**Расшифрование**

Обратная матрица ключабудет иметь вид:

8 5 10

К(^(-1)) mod 26 = 21 8 21

21 12 8

Возьмём зашифрованный текст из предыдущего примера «POH»:

8 5 10 15 0

P1=К(^(-1))\* C1mod 26 = 21 8 21 \* 14 mod 26= 2

21 12 8 7 19

**5.5. Набор для практики**

**Обзорные вопросы**

* Покажите различие между Z и Zn. Какое из этих множеств может содержать отрицательные целые числа? Как мы можем отобразить целое число в Z в целое число в Zn?
* Перечислите четыре свойства теории *делимости*, обсужденной в этой лекции. Приведите пример целого числа с единственным делителем. Приведите пример целого числа только с двумя делителями. Приведите пример целого числа с более чем двумя делителями.
* Определите наибольший общий делитель двух целых чисел. Какой алгоритм может эффективно найти наибольший общий делитель?
* Что такое линейное диофантово уравнение двух переменных? Сколько решений может иметь такое уравнение? Как может быть найдено решение(я)?
* Что такое оператор по модулю и какие у него имеются приложения? Перечислите все свойства, которые мы упоминали в этой лекции для операций по модулю.
* Определите сравнение и сопоставьте его свойства со свойствами равенства.
* Определите систему вычетов и наименьший вычет.
* Какова разница между множеством Zn и множеством Zn\*? В каком множестве каждый элемент имеет аддитивную *инверсию*? В каком множестве каждый элемент имеет мультипликативную *инверсию*? Какой алгоритм используется, чтобы найти мультипликативную *инверсию* целого числа в Zn?
* Дайте определение матрицы. Что такое матрица-строка? Что такое матрица-столбец? Что такое квадратная матрица? Какая матрица имеет *детерминант*? Какая матрица может иметь *инверсию*?
* Определите линейное сравнение. Какой алгоритм может использоваться, чтобы решить уравнение ? Как мы можем решить набор *линейных уравнений*?