Week 2: Mathematics for Cryptography I

Dr. Qublai Ali K. Mirza and Madhu Khuruna

University of Gloucestershire

hchizari@glos.ac.uk

Overview

1. Integer arithmetic
2. Integer division
3. Modular arithmetic
4. Matrices
5. Bringing it all together
6. Post-sessional work

Overview

- Refer to operations which are applied to a set of integers
- In the context of cryptography, integers contain all numbers from minus *infinity* to plus infinity
- To put this in mathematical terms, it refers to a set Z where

$$Z = \{-\infty, ..., -2, -1, 0, 1, 2, .., +\infty\}$$

Binary operations

- Binary operations in cryptography refer to operations that
  - Take as *inputs* two *integers*
  - Produce as *output* *one* *integer*
- The three binary operations we engage in cryptography are:
  - Addition $(+)$
  - Subtraction $(-)$
  - Multiplication $(\times)$

Integer division

- When dividing two integers a with b, we get two numbers namely
  - Quotient q: The result of the division
  - Remainder r: The leftover from the operation
- The relationship between a, b, q, and r can be written as:

$$a = q \times b + r$$

Division overview

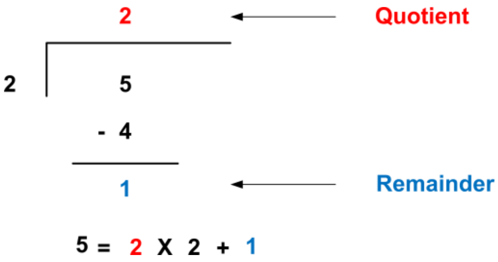

Figure: Division terms

Divisibility

- When we talk about divisibility, we are referring to cases where the remainder r is *zero*
- To express this in equation, it means:

$$a = q \times b$$

- If the remainder is zero, we write it like this: $a \mid b$
- Otherwise we write it like this: $a \nmid b$

UNIVERSITY OF GLOUCESTERSHIRE

Overview

- So far we have been looking at *integer arithmetic*, in which the result of a division operation can be express as:

$$a = q \times b + r$$

- In *modular arithmetic*, however, we are interested in one and only one of these 4 outputs: *remainder* r

Modulo operator

- Denoted by mod
- It is usually used like this where r, a, and b have the same meaning as before

$$r = a \; mod \; b$$

- For instance the following is true

$$1 = 10 \; mod \; 3$$

Exercise

- What are the moduli of the following mod operations?
  - 5 mod 26
  - 21 mod 7
  - -18 mod 14
- **Question:** what should we do if we get a *negative* modulo?

Example

Let's look at this example: -20 mod 3
By default, the answer will be this: -2 = -20 mod3, since

$$a = q \times b + r$$

$$-20 = -6 \times 3 + (-2)$$

The solution here is to reduce q by 1, and add b to r. This then becomes

$$-20 = -7 \times 3 + 1$$

Overview

- A *rectangular* array of numbers
- Organised in m *rows* and n *columns*
- Each element within the matrix is referred to as: $A = [a_{ij}]$

UNIVERSITY OF GLOUCESTERSHIRE

$$A = \begin{bmatrix} a_{11} & a_{12} & . & . & a_{1m} \\ a_{21} & a_{21} & . & . & a_{2m} \\ a_{31} & a_{31} & . & . & a_{3m} \\ . & . & . & . & . \\ . & . & . & . & . \\ a_{n1} & a_{n1} & . & . & a_{nm} \end{bmatrix}$$

Figure: Matrix structure

Operation

- Matrices are used extensively in cryptography due to their ease of:
  - Storage
  - Calculation
- We will be looking at the following matrix operations
  - Addition/Subtraction
  - Determinant
  - Inverse

UNIVERSITY OF GLOUCESTERSHIRE

Addition/Subtraction

Given two matrices

$$A = \begin{pmatrix} 3 & 4 \\ 8 & 9 \end{pmatrix}, B = \begin{pmatrix} 8 & 1 \\ 7 & 8 \end{pmatrix}$$

$$A + B = \begin{pmatrix} 3+8 & 4+1 \\ 8+7 & 9+8 \end{pmatrix}$$

$$= \begin{pmatrix} 11 & 5 \\ 15 & 17 \end{pmatrix}$$

The same principle applies for subtraction as well.

Multiplication

Given two matrices

$$A = \begin{matrix} 3 & 4 \\ 8 & 9 \end{matrix}, B = \begin{matrix} 8 & 1 \\ 7 & 8 \end{matrix}$$

$$A \times B = \begin{matrix} 3 \times 8 + 4 \times 7 & 3 \times 1 + 4 \times \\ 8 \times 8 + 9 \times 7 & 8 \times 1 + 9 \times 8 \end{matrix}$$

$$= \begin{matrix} 52 & 35 \\ 127 & 80 \end{matrix}$$

UNIVERSITY OF GLOUCESTERSHIRE

Identity matrix

- Referred to as the "1" for matrices in multiplication/divisions
- When used in multiplication, it does not change the values/positions of the original matrix
- Examples of an identity matrix are

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$I = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Inverse

- While matrix addition/subtraction are pretty straightforward, it is not that straightforward when it comes to division
- We can't use the same approach as we did with multiplication for division either
- However we found that

$$\frac{6}{2} = 6 \times 2^{-1} = 3$$

- This is known as *inverse* in matrix operations

Inverse of a matrix

- Given a matrix A, its inverse A^{-1} is a matrix such that:

$$A \times A^{-1} = I$$

- I is the *identity* matrix
- Obtained by using

$$A^{-1} = \frac{1}{det(A)} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

Determinant

- Applies to *square* matrices
  - Matrices with the same number of rows and columns (e.g., 2×2)
- Used to determine if a given matrix is *invertible*
- A matrix is *invertible* *iff* its determinant is *non-zero*

Determinant

Given a matrix A

$$A = \begin{matrix} 3 & 4 \\ 8 & 9 \end{matrix},$$

the determinant $det(A)$ is calculated as:

$$det(A) = (a \times d) - (b \times c) = (3 \times 9) - (4 \times 8) = -5$$

Getting the inverse of A

- Now that we know the determinant of A ($det(A)$), getting the inverse matrix A^{-1} is now straightforward
- The inverse of A then becomes

$$A^{-1} = \frac{1}{det(A)} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

$$= \frac{1}{(-5)} \begin{pmatrix} 9 & -4 \\ -8 & 3 \end{pmatrix}$$

$$= \begin{pmatrix} 9/5 & -4/5 \\ -8/5 & 3/5 \end{pmatrix}$$

Bringing it all together

- Today we looked at the mathematical foundations behind cryptography
- We also basics of division and more specifically remainder
- We also looked at matrices and their basic operations
- Next week: *Introduction to Cryptography II*

UNIVERSITY OF GLOUCESTERSHIRE

Post-sessional work

- Using the article “Shannon’s Theory of Secrecy” [1] as a starting point, write a critical review on how *entropy* is used in cryptography.
- You are more than welcome to use any external resources
- Submit it on Moodle for feedback by next *Thursday*

UNIVERSITY OF GLOUCESTERSHIRE

References

[1] *Shannon's Theory of Secrecy*. http://www.eit.lth.se/fileadmin/eit/courses/edi051/lecture_notes/LN3.pdf. Accessed: 2018-01-17.

Q & A