"Begin at the beginning," the King said gravely,
"and go on till you come to the end: then stop."

— Lewis Carroll, Alice in Wonderland

Project and Training 2
Mathematics Part

BSc in Computer Science
Autumn Semester 2020

Structure

The Mathematics part is divided into two independent sections - the first topic is **Relations** and the second is the **RSA-Algorithm**. To solve the exercises for the first topic, read the chapter on Relations in the *Discrete Mathematics* script of last year (to be found on moodle).

The **RSA-tasks** build upon the topics **Number Theory and Cryptography**, covered in *Discrete Mathematics I* last year. In order to complete them you will also need the two pairs of primes, the three messages and a public key that will be sent to you personally by email.

Deliverables

Relations: A single pdf-file of your solutions. Solutions written in a suitable word processing system such as LaTeX are preferred, but you may also write your solutions by hand. In the latter case, provide a proper scan of your solutions. The pdf-file containing your solutions should be uploaded into the corresponding tool in moodle.

RSA-Algorithm: Please submit your code and answers electronically via moodle.

Evaluation

The following criteria are important for the evaluation

1. Correctness of both the results and your derivations
2. Completeness of your arguments
3. Mathematical style and readability

Each of the 4 exercises on the topic of Relations can help you attain 2 points. The RSA-exercise can gain you 4 points. In total, you pass the Mathematics part if you get at least 8 out of 12 points.

Berner Fachhochschule
Haute école spécialisée bernoise
Bern University of Applied Sciences

Exercise 1 Decide, if the following relations are *reflexive, symmetric* or *transitive* on the given set A. Give a short reason in each case.

a) $R = \{(a,b) : a,b \in \mathbb{Z}, a \neq b\}$, $A = \mathbb{Z}$

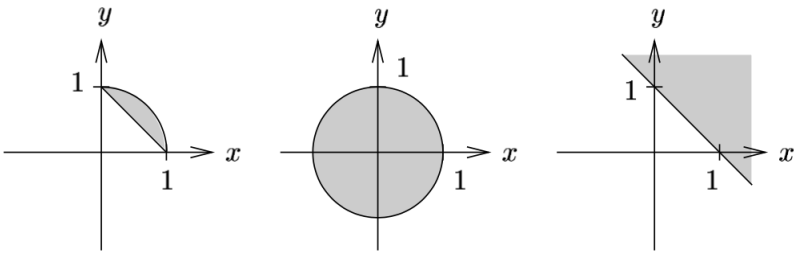
b) $R = \{(a,b) : a,b \in \mathbb{R}, a+b = 1\}$, $A = \mathbb{R}$

c) $R = \{(a,b) : a,b \in \mathbb{R}, a^2 < b^2\}$, $A = \mathbb{R}$

d) $R = \{(2,1),(3,2),(3,1)\}$, $A = \{1,2,3\}$

Exercise 2 Determine the relations $R \subseteq \mathbb{R}^2$, whose graphical representation correspond to the grey shaded areas in the images below (give one relation per figure).

Hint: First define relations for the middle and right images and then use set operations to determine the relation for the left image.



Exercise 3 Consider the set

$$\{2,4,5,10,12,20,25\}$$

with the partial order $x|y$ (in words this simply means "x divides y").

a) Draw the corresponding Hasse-Diagramm.

b) Determine the maximal and minimal elements.

c) Determine a total order that is compatible with the partial order.

Exercise 4 On the set of integers $\mathbb{Z}$ consider the following relation:

$$xRy \overset{\text{Def.}}{\Longleftrightarrow} x - y \text{ is even}$$

Prove that R is an equivalence relation and specify the corresponding equivalence classes.

Exercise 5 Using Java or Kotlin, implement the RSA algorithm for encrypting and decrypting so that the following tasks can be completed.

a) First convert your first message into ASCII and then encrypt it using the RSA algorithm using your first pair of primes. List the code with annotations, describing the main steps of the algorithm as well as the output it generated when you encoded your first message.

b) Next, code a Hash function with the second prime pair in order to sign your encoded message using your fist name converted to ASCII. List the code with annotations describing the main steps of the algorithm, and the output it generated when you hashed your first name.

c) Next decrypt your encoded message using the second pair of primes and convert it back from ASCII. List the code with annotations describing the main steps of the algorithm, and the output it generated when you decoded your second message.

d) You suspect that the public key that the encrypted third message was written in, was poorly chosen, in that the two primes used to generate it were very close together. Write the code to crack the key and decode the message. Hint: this case is discussed in the *Discrete Mathematics I* script and notes.

e) RSA is not widely used in the industry anymore. Write a brief paragraph (< 300 words) describing where RSA is still used, why it is not used as widely as before, what are some of the popular encryption methods today and what their advantages over RSA are.