Institut for Matematik og Datalogi
Syddansk Universitet, Odense

4. december 2021
JFB/DM/RF

Opgaver DM534 uge 49/50

Husk at læse de relevante sider i slides og noter før du/I forsøger at løse en opgave.

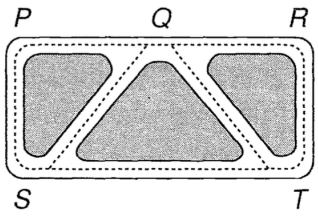
I: Løses i løbet af øvelsestimerne i uge 49

1. We consider the RSA system and use the notation and algorithms from the slides. Let $N_A = 1517$ and $e_A = 13$.

   - Encrypt the message $m = 43$. For the modular exponentiation, use the algorithm from the slides, page 38. Show all steps in your computation.
   - If you had created the keys yourself, you would know that $p = 37$ and $q = 41$. From this information and $e_A = 13$, find the secret key d_A. Use the Extended Euclidean Algorithm from pages 47–48 of the RSA slides used in lectures (there, e and d are called a and s (and d also is called x at top of page 48)). Show all steps in your computation.

2. Why in RSA is it necessary that $gcd(e_A, (p_A-1)(q_A-1)) = 1$? Find an example (that is, values e_A, p_A and q_A) where this greatest common divisor is not equal to 1.

3. Draw the graph representing the road system in the figure below, and write down the number of vertices, the number of edges and the degree of each vertex.



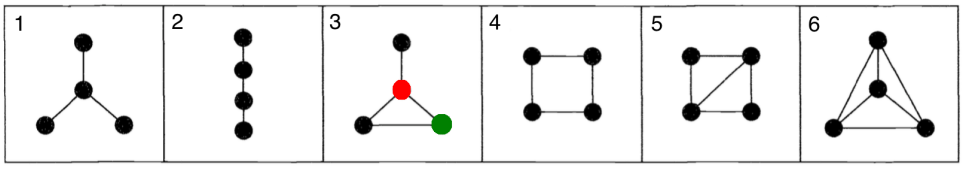
4. On Twitter:

   (a) John follows Joan, Jean and Jane; Joe follows Jane and Joan; Jean and Joan follow each other. Draw a digraph illustrating these follow-relationships between John, Joan, Jean, Jane and Joe.

   (b) Twitter has $\approx$ 313 million active users (June 2016, based on Twitter Inc.). Imagine you would like to store the digraph for the follow-relationships in an adjacency matrix that uses 4 bytes per entry on your new laptop which has 64 GB of RAM. Is this feasible?

   (c) The municipality of Odense has a population of $\approx$ 200000 people. Let G be the graph where the meaning of an edge from vertex i to j is *"person i is friends with person j"*. Imagine you would like to store the adjacency matrix for this graph for the relationships in a matrix representation that uses 4 bytes per entry on your new laptop which has 64 GB of RAM. Is this feasible?

5. Consider the following six graphs (note that the nodes do not have labels).



   (a) How many walks of length 3 from the red vertex to the green vertex are there in graph 3?

   (b) How many paths from the red vertex to the green vertex are there in graph 3?

(c) How many shortest paths from the red vertex to the green vertex are there in graph 3?

(d) For each of the graphs: what is the longest of all pairwise shortest paths?

(e) Give an adjacency matrix for graph 1. Can there be different adjacency matrices for the same graph? If so, name a second adjacency matrix for graph 1. Can you find two different adjacency matrices for graph 6?

6. Let A be an adjacency matrix. In the lecture you learned that the ij-entry of A^k is the number of different walks from vertex i to vertex j using exactly k edges.

   (a) What is the interpretation of ij-entry of the matrix $A^1+A^2+A^3$?

   (b) Complete the following sentence with the missing expression: In a graph G with adjacency matrix A, vertex i and j are connected if and only if $\ldots > 0$.

II: Løses hjemme inden øvelsestimerne i uge 50

1. Find four different square roots of 1 modulo 143, i.e., numbers which multiplied by themselves modulo 143 give 1 (and which are at least 0 and less than 143). You may consider writing a simple program for finding them.

2. Try executing the Miller-Rabin primality test on 11, 15, and 561. First, what type of numbers are they (note: 561 is known from the slides)? For each, run the Miller-Rabin test for at least one value a of your own choice, preferably for more. Use e.g. a simple Java program importing the class `BigInteger` from the Java library for executing the exponentiations (first raising to a power and then using modulus should work in reasonable time for numbers this size, hence there is no need to use the fast modular exponentiation algorithm in this exercise). Which calculations showed that the composite numbers were not prime—the first line (the Fermat test) or later lines?

   With 561, be sure to try an a relatively prime to 561 (most are, 2 is a simple example). What happens differently if you try $a = 3$? Can you explain the latter?