# Ve203 Discrete Mathematics (Fall 2016)

## Assignment 8: Counting and Probability

**Date Due: 4:00 PM, Thursday, the 24th of Noevmber 2016**

This assignment has a total of **(22 Marks)**.

### Exercise 8.1

The following is a message encoded in a fixed-substitution cipher:

19 17 17 19 14    20 23 18 19 8    12 16 19 8 3    21 8 25 18 14    18 6 3 18 8    15 18 22 18 11

By using the frequency distribution of the letters of the English alphabet and educated guessing, decipher the message.

It helps to know the context: suppose that this message was obtained from Japanese military communications in late 1941.[1]
**(3 Marks)**

### ✱ Exercise 8.2

Use the RSA algorithm with $p = 7$ and $q = 11$ as well as an exponent of $e = 7$ to encrypt the number $m = 23$.
**(3 Marks)**

### Exercise 8.3

Let $G$ be a cyclic group and $g \in G$ be a generator. Prove that $G$ is abelian.
**(2 Marks)**

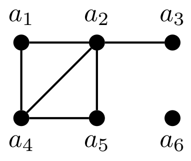
### ✱ Exercise 8.4

Alice and Bob have used the Diffie-Hellmann protocol to establish a common secret key. They have used the multiplicative group $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$ (which has multiplication modulo 7 as group operation) and the generator $g = 3$. Alice has sent the number 6 to Bob and Bob has sent the number 5 to Alice. What is their common secret key?
**(2 Marks)**

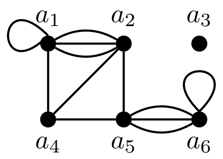
### ✱ Exercise 8.5

In the following graphs, find the number of vertices, the number of edges and the degree of each vertex. Identify all isolated and pendant vertices. Classify each graph as a simple graph, a multigraph or a pseudograph. Give the adjacency matrix for each graph.

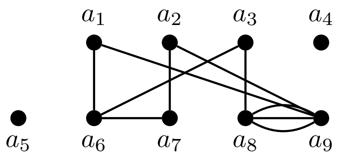
i)



ii)



iii)

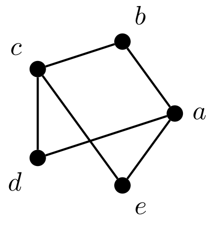


**(6 Marks)**

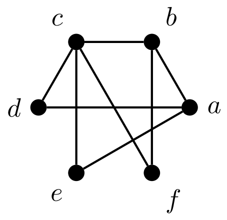
### ✱ Exercise 8.6

In the following graphs, determine which ones are bipartite and give a bipartition for those that are.

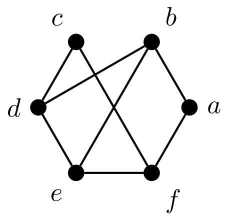
i)



ii)



iii)



**(3 Marks)**

[1] This question uses a message from Neal Stephenson's bestseller *Cryptonomicon*, a highly readable book for the holidays. The solution can also be found in the book.

### Exercise 8.7

An *intersection graph* for a collection of sets $A_1, \dots, A_n$ is the graph $G = (V, E)$ with $V = \{A_1, \dots, A_n\}$ and $E = \{\{A_i, A_j\} \colon A_i \cap A_j \neq \emptyset\}$. Draw the intersection graphs for the followings sets:

i) $A_1 = \{0, 2, 4, 6, 8\}$, $A_2 = \{0, 1, 2, 3, 4\}$, $A_3 = \{1, 3, 5, 7, 9\}$, $A_4 = \{5, 6, 7, 8, 9\}$, $A_5 = \{0, 1, 8, 9\}$.

**(1 Mark)**

ii) $A_1 = \mathbb{Z} \setminus \mathbb{Z}_+$, $A_2 = \mathbb{Z}$, $A_3 = 2\mathbb{Z}$, $A_4 = 2\mathbb{Z} + 1$, $A_5 = 3\mathbb{Z}$. (Notation is analogous to Example 1.3.5 in the lecture slides.)

**(1 Mark)**

iii) $A_1 = (-\infty, 0)$, $A_2 = (-1, 0)$, $A_3 = (0, 1)$, $A_4 = (-1, 1)$, $A_5 = (-1, \infty)$, $A_6 = \mathbb{R}$. (All sets are intervals in $\mathbb{R}$.)

**(1 Mark)**

**(3 × 1 Mark)**

### Exercise 8.8

Complete the IDEA survey for Ve203.
**(5 Bonus Marks)**