UNIVERSITY OF OSLO

Faculty of mathematics and natural sciences

Exam in:	MAT2250 — Discrete Mathematics
Day of examination:	Wednesday 2. June 2021
Examination hours:	9:00 – 13:00
This problem set consists of 3 pages.	
Appendices:	none
Permitted aids:	all

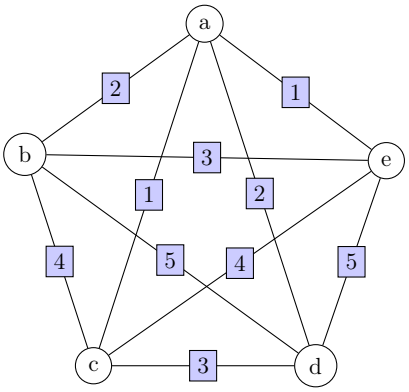
Please make sure that your copy of the problem set is complete before you attempt to answer anything.

Justification must be provided for all solutions. Solutions can be submitted in English or Norwegian. The format may be in Latex or as scanned handwritten notes.

Problem 1 25 points

1. (5 points) For what n is the complete graph K_n Eulerian?

   Consider the traveling salesperson problem (TSP) on the above graph where the number on an edge indicates its weight.



2. (5 points) Is this a metric TSP?

3. (15 points) Run the Christofides heuristic to provide a route for a traveling salesperson. Explain each step of the heuristic and name the graph algorithms that you use as they arise.

Problem 2 25 points

1. (5 points) Consider the 2-design with $v = 7$ consisting of the blocks

$$\mathcal{B} = \{\{123\}, \{137\}, \{156\}, \{235\}, \{267\}, \{346\}, \{457\}\}.$$

(Continued on page 2.)

Write down the $v \times b$ incidence matrix of the design. What are the values of the parameters k and λ for this design?

2. (10 points) From a t-block design with parameters $v, k, \lambda = 1$ construct a binary code with $|C| = |\mathcal{B}|$ and satisfying $d(C) \geq 2k - t + 1$.

   Hint: use the columns of the incidence matrix of the design as the code words.

3. (10 points) For $a \in \{0,1\}^n$ find and prove a formula for the number of points in

$$B_t(a) = \{b \in \{0,1\}^n \mid \Delta(a,b) \leq t\} \subseteq \{0,1\}^n$$

   where $\Delta(a,b)$ denotes the Hamming distance.

   Use inclusion-exclusion to determine the number of points in

$$B_1((0,0,0)) \cup B_1((1,0,0)) \cup B_1((0,1,0)).$$

Problem 3 25 points

1. (5 points) Let $C \subset \{0,1\}^5$ be the binary linear code

$$C = \{00000, 11100, 11111, 00011\}.$$

   Write down a generating matrix for C.

2. (10 points) Let $C \subset \{0,1\}^8$ be the binary cyclic code of dimension 4 generated by the polynomial:

$$g(x) = x^4 + 1.$$

   Using the generating polynomial, encode the words $a = (1,0,1,0)$ and $d = (1,1,1,1)$.

   While using the above cyclic code, you receive the transmission $(0,0,1,0,1,1,1,1) \in \{0,1\}^8$. Use the fact that the code is cyclic to show that an error has occurred.

3. (10 points) Show that the cyclic code from part 2 is self-dual, namely that $C = C^{\perp}$.

Problem 4 25 points

1. (5 points) Use Fermat's little theorem to compute 3^{302} modulo 5.

2. (10 points) Solve the discrete logarithm problem

$$3 \equiv 7^x \mod 11$$

   for $x \in \{0,1,\ldots,10\}$.

   Find elements $a, y \in \mathbb{Z}_5$ such that

$$y \equiv a^x \mod 5$$

   does not have a unique solution for $x \in \{0,1,2,3,4\}$.

(Continued on page 3.)

3. (10 points) Alice and Bob exchange encrypted messages using the RSA protocol. However, Eve and Iver set out to interfere with the transmission. Using the public key $n = 187$ and $k = 7$, Bob sends an encrypted message to Alice asking if she wants to meet.

   First Eve cracks Bob's private key by factoring $n = 187$ and using the Euclidean algorithm. Find Bob's private key using the same method as Eve.

   Using the private key they decode the message, then using Alice's public key $n' = 91$ and $k' = 5$, Iver poses as Alice and encrypts the message "NO" using the encoding $N = 14, O = 15$. What numbers does Iver send?

Problem 5 10 points

Provide an example of where we borrowed tools from other areas of mathematics (for example, linear algebra, analysis, or abstract algebra) to solve discrete problems. Describe how the theorem/fact/construction borrowed from the other area produced results about discrete objects.