UNIVERSITY OF OSLO

Faculty of mathematics and natural sciences

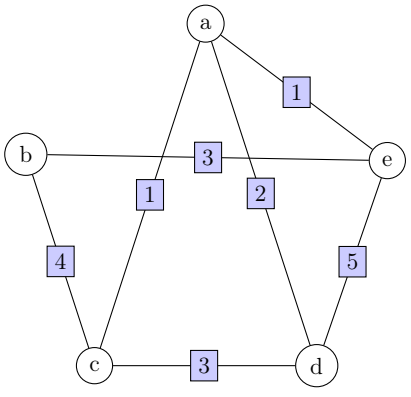
Exam in:	MAT2250 — Discrete Mathematics
Day of examination:	**Practice Exam 2021**
Examination hours:	00:00 – 04:00
This problem set consists of 2 pages.	
Appendices:	none
Permitted aids:	all

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) Find a Hamiltonian cycle in the hypercube graph Q_3.
2. (10 points) Find and prove a formula for the number of Hamiltonian cycles of K_n.
3. (10 points) Solve Kwan Mei-Ko's postal route problem (known as the Chinese postman in Aigner) for the weighted graph below starting at vertex a. The numbers along the edges indicate their weights.



Problem 2 25 points

1. (10 points) Suppose in a finite projective plane of order n any three non-collinear points form a triangle. Show that the number of triangles is
$$\frac{1}{6}n^3(n+1)(n^2+n+1).$$

(Continued on page 2.)

2. (10 points) Given a finite projective plan of order n construct $n-1$ orthogonal Latin squares of order n. Explain how the orthogonality of the Latin squares constructed follows from the axioms of the finite projective plane.

3. (5 points) Use Problem 2.2 to justify that there is no finite projective plane of order 6.

Problem 3 25 points

1. (5 points) Is the code

$$C = \{000000, 111000, 111111, 000111, 101010, 010101\} \subset \{0,1\}^6$$

linear?

2. (10 points) Let $C \subset \{0,1\}^7$ be a linear code with parity check matrix

$$H = \begin{pmatrix} 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \end{pmatrix}$$

What is the dimension of C?

In a transmission you receive the code word $c = (1,1,1,1,0,0,0)$. Show that an error occurred.

3. (10 points) Suppose you want to construct a binary 2-error correcting code C with $|C| = 4$. Hamming's bound gives a lower bound on the possible length of the code. What is this bound?

Problem 4 25 points

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

2. (5 points) Show that 2 is a primitive root modulo 11.

3. (10 points) In a Diffie-Hellman key exchange Alice and Bob share the public key $p = 11$ and $a = 2$. Alice sends $A = 10$ to Bob and Bob sends $B = 6$ to Alice. What is their shared secret key K?

The ElGamal protocol which encrypts a text T to a cipher

$$C \equiv KT \mod p.$$

Using the ElGamal protocol with their public keys and shared secret, Bob sends the number $C = 6$ to Alice. What was the original number T?

Problem 5 10 points

Our course consisted of three main sections, enumerative combinatorics, graph theory, and algebraic structures. Provide an instance of when at least two of these sections overlapped, and illustrate your claim with a concrete example.