SOLUTIONS of Final Exam – Part A and B – SF1610 Discrete Mathematics – TCOMK

Examiner: Armin Halilovic
Course responsible: Ivan Martino
Date: 2020-05-27

Part A and B – Time: 8:00 – 11:00 (Extra-time students: 8:00 – 12:30)
Right after, you have 20 minutes to take pictures and upload your solution on Canvas.
Part C will be sent to you later. Time: 11:30 – 13:30 (Extra-time students: 13:00 – 16:00)

Short summary of the rules of the exam:

1. Use your computer only to read the questions of the exam.
2. If you may, use your phone for the Zoom-meeting call and place it so that your desk is visible; if you are not using your phone for the Zoom-meeting call, then you cannot use your phone for the whole exam.
3. No calculator, books, notes, lecture notes are allowed.
4. You may use your phone during the 20 minute break to take picture of your solution. You still need to be visible while doing so, hence you need to be in the Zoom-call from another device.

The exam consists of 10 questions in three parts: A, B and C. **Problems are not ordered by difficulty.** This exam provides a total of 39 points, plus any extra bonus points from the partial exams. The bonus point collected during the semester will be extra to the final exam score.

IMP. The full points will be given only to complete and fully explained solutions.

Evaluation table:
13 points total or more – give at least the grade of Fx
15 points total or more – give at least the grade of E
18 points total or more – give at least the grade of D
22 points total or more – give at least the grade of C
27 points total or more – give at least the grade of B
32 points total or more – give at least the grade of A

You should use paper and pen to solve the following exercises. You scan/take pictures of your solutions (jpg, jpeg, png, pdf format). Then, you have to upload your solutions gathered in a folder and compressed (as a zip or rar file) to Canvas / tasks / Final Exam – May 27, 2020 – Part 1: A and B.

Extra-time students should use a different folder Canvas / tasks / Final Exam – May 27, 2020 – Part 1: A and B – Extra time students.

IMPORTANT: The folder name should contain your last name and name; in other words use the NAME_FIRSTNAME as name of the folder with your solutions.

Write names and social security numbers on each sheet. On the first sheet write "I have done this Final exam by myself" and sign it. So you declare that you have made final exam by yourself.

The parameters p and q in the information below are the last two digits of your social security number. For example: If your social security number is 751332 2248 then p = 4 and q = 8.

PART A – If you have passed all partial exams, move to PART B.

1. (3p) Determine all integer solutions (x, y) of the Diophantine equation
$(q+3)x + (10-q)y = -q^2 + 7q + 30$.
IMP. Only a full explained complete solution will get points.

Solution for q=9.

For q=9, the equation is 12x+y=12 and since the GCD of the coefficients is one, GCD(12,1)=1, the equation has solution. In particular, the pair $x_0 = 0$ and $y_0 = 12$ is a solution. On the other, hand we know that we gain all the solutions, by adding a generic solution to 12x+y=0, that is x=k, y=-12k for every integer k. Hence we get:

x= 0 + k, y = 12 – 12k, for every integer k.

Alternatively, we can also use Euclide's Algorithm and find solution for the equation 12x+y=1, then multiply such solution for 12.

SOLUTION FOR q = 9: x= 0 + k, y = 12 – 12k, for every integer k.

SOLUTUON FOR ANY q.

q = 0, 3*x+10*y = 30 , GCD(a,b)= 1, Lösning:{x = 10-10*k, y = 3*k}

q= 1, 4*x+9*y = 36 , GCD(a,b)= 1, Lösning:{x = 9-9*k, y = 4*k}

q= 2, 5*x+8*y = 40 , GCD(a,b)= 1, Lösning:{x = 8-8*k, y = 5*k}

q= 3, 6*x+7*y = 42 , GCD(a,b)= 1, Lösning:{x = 7-7*k, y = 6*k}

q= 4, 7*x+6*y = 42 , GCD(a,b)= 1, Lösning:{x = 6*k, y = 7-7*k}

q= 5, 8*x+5*y = 40 , GCD(a,b)= 1, Lösning:{x = 5*k, y = 8-8*k}

q= 6, 9*x+4*y = 36 , GCD(a,b)= 1, Lösning:{x = 4*k, y = 9-9*k}

q= 7, 10*x+3*y = 30 , GCD(a,b)= 1, Lösning:{x = 3*k, y = 10-10*k}

q= 8, 11*x+2*y = 22 , GCD(a,b)= 1, Lösning:{x = 2*k, y = 11-11*k}

q= 9, 12*x+y = 12 , GCD(a,b)= 1, Lösning:{x = k, y = 12-12*k}

Grading: a correct first solution gets 1p

+1p for correct values of x

+1p for correct values of y

2. (3p) Find all integers n such that $100 + p \leq n \leq 200 + p$ which are divisible by 3 or 4.

Note. For instance, n=123 is one of such numbers because it is divisible by 3.
IMP. Only a full explained complete solution will get points.

SOLUTIONS FOR p=9.

We should find all integers *n*, such that $109 \le n \le 209$, which are divisible by 3 or 4.

We use inclusion-exclusion principle.

Remeber that our groud set is U={109,110, …208,209} and we denote by

A: the set of all integers n such that $109 \le n \le 209$ that are divisible by 3.
B: the set of all integers n such that $109 \le n \le 209$ that are divisible by 4.

The union $A \cup B$ is made by all integers in U divisible by 3 or 4.

Let |M| be the cardinality of a set M.

Using inclusion-exclusion principle, we know
$|A \cup B| = |A| + |B| - |A \cap B|$

We compute |A| as

$$\left[\frac{209}{3}\right] - \left[\frac{108}{3}\right] = 69 - 36 = 33 .$$

And |B| as

$$\left[\frac{209}{4}\right] - \left[\frac{108}{4}\right] = 52 - 27 = 25 .$$

Finally, the intersection $|A \cap B|$ is made by all intergers in U that are divisible by 3 and 4, so divisible by 12; hence the cardinality of the intersection is

$$\left[\frac{209}{12}\right] - \left[\frac{108}{12}\right] = 17 - 9 = 8 .$$

We can pach things together and we get:

$|A \cup B| = |A| + |B| - |A \cap B|$ =33+25–8=50.

Grading:

1p for correct inclusion exclusion form

2p for correct inclusion exclusion form and correct computation of |A|, |B| and $|A \cap B|$ $|A \cap B|$ 3p all correct.

3. (3p) Let n = 5p + 15 and consider the group G = (Z/n, +)
3.a) Determine a subgroup H to G such that |H| = p + 3.
3.b) Determine all cosets of H.
3.c) Determine an element in the group (Z/n, +) that has order 5.
Note: in item 3.c) you need to find only one element, you don't need to list all of them.

a) SOLUTION FOR P=9:

We have n=5·9+15 =60 and so we work with the group G=(*Z/60,* +)

We should find the subgroups of order 9+3= 12.

Let H be the cyclic subgroup generated by the element 5.

Hence, we get that H is made by the following elements: 0, 5, 5+5=10, 5+5+5, 5+5+5+5… , 55. Shortly, H={0,5,10, …55} and has order 12.

a) SOLUTION: H={0,5,10, …55}

a) GENERIC SOLUTION. H=<5>.

b) SOLUTION FOR p=9:

Since 60=12*5, there are 5 cosets of H

H+0= H={0,5,10,…,55},

H+1 ={1,6,11,…,56} ,

H+2 ={2,7,…, 57},

H+3={3,8,…, 58} and

H+4={4,9,…, 59}.

b) Generic Solution: H, H+1 , H+2, H+3 and H+4

c) **SOLUTION FOR p=9:**

We should find an element in (Z/60, +) that has order 5.

Let a=12 and compute 12+12 =24, …   12+12+12+12+12 =0   (in the group (*Z/60*, +)) .

Hence, a=12 has order 5.

c) Solution: 12.

c) Generic solution: p+3.

Grading

1p for each item

4. (3p) Let A = p mod 2.
4.a) Find all the words of the linear binary code defined by the matrix

$$H = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & A & 1 \\ 0 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

4.b) Find the minimal distance between two words of the above defined code.
IMP. Only a full explained complete solution will get points.

Lösning för A=0

a)

$$H = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

All the words in the code are of lenght 5, $(x_1, x_2, x_3, x_4, x_5)$, and they are solution of the following linear system:

$$H = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}.$$

By Gauss elimination we get that

$$\left[\begin{array}{ccccc|c} 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 \end{array}\right] \sim (R1+R2) \left[\begin{array}{ccccc|c} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 \end{array}\right] \sim$$

$$\text{byta pl. R2,R3} \left[\begin{array}{ccccc|c} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \end{array}\right]$$

Thus, we have two free parameters x_4, x_5 that can describe the remaining variables x_1, x_2, x_3 as:

$x_3 = x_4$, $x_2 = x_5$ och $x_1 = x_4 + x_5$

The parameters x_4, x_5 can take values 0 or 1 (Table A) and therefore we have only 4 words in the code.

Table A:

(x_1,x_2,x_3,x_4,x_5)	
0	0
0	1
1	0
1	1

Table B:

(x_1,x_2,x_3,x_4,x_5)				
0	0	0	0	0
1	1	0	0	1
1	0	1	1	0
0	1	1	1	1

Answer for A=0

a) The code has four words

(0,0,0,0,0), (1,1,0,0,1), (1,0,1,1,0), (0,1,1,1,1)

b) The minimal distance is 3.

Answer for A=1

The linear system is $x_1 = x_4 + x_5$, $x_2 = x_4 + x_5$, $x_3 = 0$ $x_3 = 0$

a) The code has four words

(0,0,0,0,0), (1,1,0,0,1), (1,1,0,1,0), (0,0,0,1,1)

b) The minimal distance is 2.

Grading

a) 1 p for correct linear system ($x_1 = x_4 + x_5$, $x_2 = x_5$, $x_3 = x_4$).

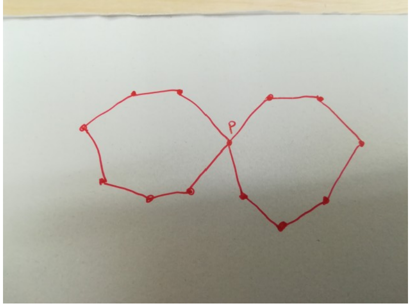
2 p, everything correct.

b) 1p for correct answer

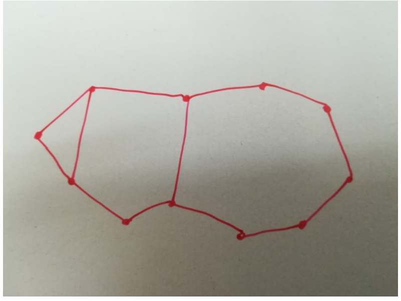
5. (3p) Draw a connected graph with at least (p + 5) edges...
5.a) which is Eulerian but not Hamiltonian graph.
5.b) which is Hamiltonian graph but not Eulerian graph.
5.c) which is neither Eulerian nor Hamiltonian graph.
Note. The number of edges of the graph is larger or equal to (p+5).
Note. You have to draw, if possible, three graphs; one for each item of the exercise.
IMP. Only a full explained complete solution will get points.

Solution.

a) we need to provide only an example of Eulerian graph that is not Hamiltonian. Eulerian, means the degree of every vertex is even, while for being Hamiltonian, No matter how we walk through all nodes, we must pass node P at least twice.

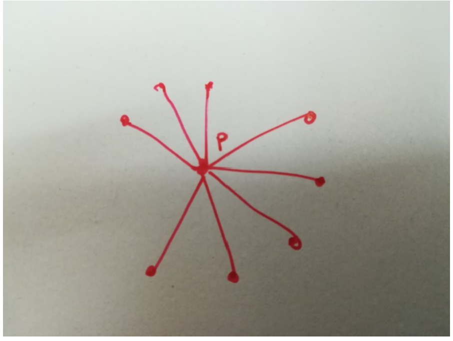


b) we need to provide only an example of an Hamiltonian Graph that is not Eulerian. We consider a large cycle and we connect four verticies in pair so that there are 4 verticies with odd degrees, which means that the graph is not Eulerian.



c) we need to provide only an example of a graph that which is neither Eulerian nor

Hamiltonian. Hence consider the star graph just below. This is not Eulerian, because every verticies, different from P, has odd degree. (This may happen also at P.) Not Hamiltonian, because to walk over the graph you must pass several times through P.



Grading:

1p for each item.

PART B – If you have passed all partial exams, you start here.

6. (4p)
Show using the induction method that

$$q\cdot 3^{2n+3}+27\cdot 9^{n}+(q+1)\cdot(40n-27)$$

is divisible by 64 for all integers n with $n\geq 0$.
IMP. You get no point if you do not use the induction method.

Solution.

To simplify calculation, we factor the expression

$$q\cdot 3^{2n+3}+27\cdot 9^{n}+(q+1)\cdot(40n-27)$$
$$=q\cdot 3^{2n+3}+3^{2n+3}+(q+1)\cdot(40n-27)$$
$$=(q+1)\cdot(3^{2n+3}+40n-27)$$

Now, we will prove that 64 divides $3^{2n+3}+40n-27$ for any n

(You may use directly the induction method without factizing the expression.)

a) Induction Base

For $n=0$ we get $3^{0+3}+40\cdot 0-27=27-27=0$ that is divisible by 64.

b) Induction Step.

Consider a specific integer n. The statement, *P*(*n*), is that

$3^{2n+3}+40n-27$ =64c (*) ,

for a certain integer c. We want to prove that *P*(*n*+1) holds, that is
$3^{2n+5}+40(n+1)-27$ = 64d, for a certain integer d.

From the induction hypothesis we get $3^{2n+3}+40n-27$ =64c, and so

$3^{2n+3}=64c-40n+27$ (**) .

Let us focus on the left hand side (VL) of P(n+1).

$VL=3^{2n+5}+40(n+1)-27=3^{2}3^{2n+3}+40(n+1)-27$
And using (**)

VL=3^2(64c -40n +27)+40(n+1) – 27 = 9*64c - 9*40n + 9*27+ 40 n + 40 – 27=

= 9*64c - 8*40n + 8*27+ 40 = 9*64c – 320 n + 8*27+ 8*5= 9*64c – 320 n + 8*32=

=64(9c – 5n + 4).
Hence $P(n)\Rightarrow P(n+1)$ with d= 9c-5n+4.

From a) and b), using the mathematical induction, we get that the statement hold for very integer with $n \geq 0$.

Grading Table:
1p correct use of the induction method (correct base, correct induction statement)
1p for correct verification of the induction base
2p for correct induction proof.

7. (4p)
7.a) (2p) Let K = 7+ (p mod 2). Determine the number of words of length K that can be formed using the letters a, b, c, d and e, such that each of the letters a, b, c and d occur at least once in the word, while the letter e occurs exactly twice in the word.

a) Solution for K=8:

Step 1. First we choose two places for the letter e. We can do this in $\binom{8}{2}$ ways.
Step 2. Then we divide the remaining 6 places on the letters a, b, c and d. We can do this in

4! * S (6.4) way, where S (6.4) is Stirling number. So the total number is 4! *S(6,4) * $\binom{8}{2}$.

Answer a)

For K=8 the solution is 4! *S(6,4) * $\binom{8}{2}$ =43680.

For K=7 the solution is 4! *S(5,4) * $\binom{7}{2}$ =5040.

Alternative solution: There is a very natural notations that could be used in this case and it is also well described in the book: the multinomial coefficient. Using this, it is almost immediate to say that K = 8, the solution is 4*(8 choose 2,3,1,1,1) + (4 choose 2)(8 choose 2,2,2,1,1); for K = 7 we have 4*(7 choose 2,2,1,1,1).

7.b) (2p) In one class there are (20 + q) students from Stockholm, 12 students from Uppsala and 14 students from Sundsval. You want to select a team that contains 7 students, which includes at least one student from each of the three cities. Determine the number of such teams (with 7 students and at least 1 from each city).
Also, determine the number of such teams (with 7 students and at least 1 from each city) where the number of students from Stockholm is greater than the number of students from Uppsala and Sundsval together.

Note. In assignment 7.a and 7.b, you may use the binomial coefficient and Stirling number notations in the answer.
IMP. Only a full explained complete solution will get points.

b) Solution for q= 9.

We want to determine the numbers of teams with 7 students and and at least 1 from each city. We have (20+q) students from Stockholm, 12 students from Uppsala and 14 students from Sundsval. In other words, in the team we want a total of 7 students and at least one should come from Stockholm (20+q possibilities), one from Sundsval (12 possibilities) and one form Uppsala (14 possibilities).

There are a total of (46+q choose 7) teams, and we need to remove the ones where all students comes from only two cities, that includes the case where all students come from a singlie city; this number is (32+q choose 7) + (34+q choose 7)+ (26 choose 7). Finally, we observe that in the latter computation we are double counting the single city teams, hence we add back (20+q choose 7) + (12 choose 7) + (14 choose 7). This leads to the following solutions:

Answer: (46+q choose 7) + (20+q choose 7) + (12 choose 7) + (14 choose 7) - (32+q choose 7) - (34+q choose 7) - (26 choose 7). (*)

Now, we want to compute the total number of such teams, with a larger number of Students form Stockholm. If 4 places taken by Stockholmian then we have (20+q over 4)*[12*(14 over 2) + 14*(12 over 2)]. To this number we are going to sum the number of teams where 5 places are taken by Stockholmian, then we have (20+q over 5)*12*14.

Since we need a students by Sundsval and one from Uppsala, we cannot get 6 or 7 students from Stockholm.

Grading:
-1p for correct the ways of choosing the letter e, for item a.
-2p for all correct, for item a.
-1p for (*) in item b,
-2p for the full answer in item b.

8. (4p)

An RSA-method has the following parameter, n = 143. Select an appropriate encryption key e where $12 \leq e \leq 20+p$. For such encryption key e, find the decryption key d. Finally, encrypt the message “2”.
IMP. Only a full explained complete solution will get points.

Solution.

First we factorize n = 143 =11*13.

Now we can compute the parameter m as m =10*12=120.

The encryption key should be choose such that $12 \leq e \leq 20+p$ and it shold be a number coprime with m =120.

So we can pick for example e =13 and find its inverse in Z/120, by solving the following Diofantine equation:
$13x = 1 + 120y$ that is

$13x - 120y = 1$.

We should of course, pick a solution among 0 and 119, i.e. $0 < x \leq 119$ and we get x=37. This is our decryption key, *d*=37.

To encrypt the message ”2” we need only to perform the following computation $2^e \bmod n = 2^{13} \bmod 143 = 41$.

ANSWER: The encrypted message for e=13 is 41.

If e = 17 then d = 113 and the encrypted message is 84;

If e = 19 then d = 19 and the encrypted message is 50.

Grading:
-1p for factorization and for m=120
-2p for correct d
-1p for correct encrypted message.