Linköpings universitet
Matematiska institutionen
Algebra, geometri och diskret matematik

Kurskod: TATA82
Modul: TEN1

Tentamen i TATA82 Diskret matematik

2024-08-22 kl 8.00–13.00

Inga hjälpmedel. Ej räknedosa.

På del A (uppgift 1–3) ska endast svar ges. De ska lämnas på ett gemensamt papper. *Varje uppgift på del A ger högst 1 poäng. Uppgifterna på del B (uppgift 4–8) ger högst 3 poäng per uppgift. Till dessa krävs fullständiga lösningar.*

Godkänt på alla tre kontrollskrivningar *KTR1–3 år 2024 adderar 1 bonuspoäng till totalpoängen. Markera detta genom att skriva "G" i rutan för uppgift 9 på skrivningsomslaget.*

För betyg 3/4/5 krävs 9/12/15 poäng totalt.

Lösningsförslag finns efter skrivtidens slut på kursens hemsida.

DEL A

1. Hur många delmängder till $\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ innehåller exakt två udda tal och minst ett jämnt tal?

2. Bestäm den största gemensamma delaren till 391 och 598.

3. Rita en enkel graf på fem hörn som är sammanhängande och eulersk men inte hamiltonsk.

DEL B

4. I ett RSA-kryptosystem har Bob den offentliga nyckeln $(33, 3)$.
   (a) Finn Bobs privata nyckel och använd den för att avkryptera kryptotexten "16".
   (b) Kontrollera att ditt resultat i (a) var rätt genom att kryptera klartexten du fann och visa att resultatet blir 16.

5. Grafen $G = (V, E)$ ges av $V = \{1, 2, 3, 4\}$, $E = \{\{1, 2\}, \{2, 3\}, \{2, 4\}\}$.
   (a) Hur många delgrafer till den kompletta bipartita grafen $K_{8,9}$ är isomorfa med G?
   (b) Hur många delgrafer till den kompletta grafen K_{10} är isomorfa med G?

6. Lös rekursionsekvationen $a_{n+2} = 3a_{n+1} + 4a_n + 18n - 9$, $n \in \mathbb{N}$, med begynnelsevärdena $a_0 = 7$ och $a_1 = 9$.

7. Hur många positiva heltal $N \leq 1800$ uppfyller att inget av talen $\frac{N}{8}$, $\frac{N}{18}$ och $\frac{N}{30}$ är ett heltal?

8. Låt $n \in \mathbb{Z}_+$ och $P_n = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} : 0 \leq a \leq b \leq n\}$. Relationen $\preceq$ på P_n definieras genom att låta $(a_1, b_1) \preceq (a_2, b_2)$ betyda att $a_1 \leq a_2$ och $b_1 \geq b_2$. (*Notera olikheternas riktningar!*)
   (a) Visa att $\preceq$ är en partialordning på P_n.
   (b) Rita Hassediagrammet för $(P_3, \preceq)$.

(ENGLISH VERSION ON OPPOSITE PAGE)

Linköpings universitet
Matematiska institutionen
Algebra, geometri och diskret matematik

Course code: TATA82
Module: TEN1

Examination in TATA82 Discrete mathematics

2024-08-22 at 8.00–13.00

No aid. No calculator.

In part A (problems 1–3), only answers shall be given. They are to be handed in on a single sheet of paper. *Each problem in part A is worth 1 point. The problems in part B (problems 4–8) are worth 3 points each. For them, complete solutions are required.*

Having passed all three digital tests *KTR1–3 in 2024 adds 1 bonus point to the total score. Indicate this by typing "G" in the box representing problem 9 on the exam cover.*

For grade 3/4/5 is required a total of 9/12/15 points.

After the exam, solutions are available from the course webpage.

PART A

1. How many subsets of $\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ contain exactly two odd numbers and at least one even number?
2. Find the greatest common divisor of 391 and 598.
3. Draw a simple graph on five vertices which is connected and eulerian but not hamiltonian.

PART B

4. In an RSA cipher, Bob has the public key $(33, 3)$.
   (a) Find Bob's private key and use it to decrypt the ciphertext "16".
   (b) Verify that your result from (a) was correct by encrypting the plaintext you found and demonstrate that the result is 16.
5. The graph $G = (V, E)$ is given by $V = \{1, 2, 3, 4\}$, $E = \{\{1, 2\}, \{2, 3\}, \{2, 4\}\}$.
   (a) How many subgraphs of the complete bipartite graph $K_{8,9}$ are isomorphic to G?
   (b) How many subgraphs of the complete graph K_{10} are isomorphic to G?
6. Solve the recurrence equation $a_{n+2} = 3a_{n+1} + 4a_n + 18n - 9$, $n \in \mathbb{N}$, with the initial values $a_0 = 7$ and $a_1 = 9$.
7. How many positive integers $N \leq 1800$ satisfy that none of the numbers $\frac{N}{8}$, $\frac{N}{18}$, and $\frac{N}{30}$ is an integer?
8. Let $n \in \mathbb{Z}_+$ and $P_n = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} : 0 \leq a \leq b \leq n\}$. The relation $\preceq$ on P_n is defined by letting $(a_1, b_1) \preceq (a_2, b_2)$ mean that $a_1 \leq a_2$ and $b_1 \geq b_2$. (*Note the directions of the inequalities!*)
   (a) Show that $\preceq$ is a partial order on P_n.
   (b) Draw the Hasse diagram of $(P_3, \preceq)$.

(SVENSK VERSION PÅ OMSTÅENDE SIDA)

Solutions

1. Construct such a subset by first choosing its two odd numbers in $\binom{5}{2} = 10$ ways, and then its even numbers in $2^4 - 1 = 15$ ways. **Answer:** 150.

2. Either observe the prime factorizations $391 = 17 \cdot 23$, $598 = 2 \cdot 13 \cdot 23$, or else apply Euclid's algorithm to find $\gcd(391, 598) = 23$. **Answer:** 23.

3. A graph obtained by gluing two 3-cycles together at a common vertex v is eulerian since, starting at v, we may first traverse the first 3-cycle and then the second. It is not hamiltonian because deleting v disconnects the graph. **Answer:** 

4. (a) Since $33 = 3 \cdot 11$, Bob's private key d is the inverse of 3 modulo $(3-1) \cdot (11-1) = 20$. Observing $3 \cdot 7 \equiv 1 \pmod{20}$ leads to the conclusion $d = 7$. We decrypt:

$$16^7 = 2^{28} = 32^5 \cdot 8 \equiv (-1)^5 \cdot 8 = -8 \equiv 25 \pmod{33}.$$

Answer: key: 7, plaintext: 25.

(b) Encrypting 25 using Bob's public key yields

$$25^3 \equiv (-8)^3 = -8 \cdot 64 \equiv -8 \cdot (-2) = 16 \pmod{33},$$

as expected.

5. Note that G is a tree with three leaves and one vertex of degree three.

(a) Such a subgraph is uniquely determined by choosing the three leaves in one of the parts of the bipartition and then the remaining vertex in the other part. Hence, there are $\binom{8}{3} \cdot 9 + \binom{9}{3} \cdot 8 = 56 \cdot 9 + 84 \cdot 8 = 1176$ such subgraphs. **Answer:** 1176.

(b) Construct a subgraph isomorphic to G by first choosing its four vertices and then selecting which of the four should be the non-leaf. Thus, there are $\binom{10}{4} \cdot 4 = 840$ possibilities. **Answer:** 840.

6. The characteristic polynomial is $x^2 - 3x - 4 = (x+1)(x-4)$. Hence, the homogeneous part of the solution is $a_n^{\text{hom}} = C_1 \cdot (-1)^n + C_2 \cdot 4^n$ for constants C_1 and C_2.

Looking for a particular solution, we make the ansatz $a_n^{\text{part}} = An + B$ which, when inserted in the recurrence, yields

$$A(n+2) + B = 3A(n+1) + 3B + 4An + 4B + 18n - 9,$$

with the unique solution $A = -3$, $B = 2$. Hence, the general solution to the recurrence equation is $a_n = C_1 \cdot (-1)^n + C_2 \cdot 4^n - 3n + 2$. The initial values impose the conditions

$$\begin{cases} 7 &= C_1 + C_2 + 2, \\ 9 &= -C_1 + 4C_2 - 1, \end{cases}$$

meaning that $C_1 = 2$, $C_2 = 3$. **Answer:** $a_n = 2 \cdot (-1)^n + 3 \cdot 4^n - 3n + 2$.

7. For $m \in \mathbb{Z}_+$, let $A_m = \{N \in \mathbb{Z}_+ : N \leq 1800 \text{ and } m \text{ divides } N\}$. Then, we wish to compute $|A_1 \setminus (A_8 \cup A_{18} \cup A_{30})|$. By the principle of inclusion-exclusion, this quantity equals

$$\begin{aligned}
&|A_1| - |A_8| - |A_{18}| - |A_{30}| + |A_8 \cap A_{18}| + |A_8 \cap A_{30}| + |A_{18} \cap A_{30}| - |A_8 \cap A_{18} \cap A_{30}| \\
&\quad = |A_1| - |A_8| - |A_{18}| - |A_{30}| + |A_{72}| + |A_{120}| + |A_{90}| - |A_{360}| \\
&\quad = 1800 - \frac{1800}{8} - \frac{1800}{18} - \frac{1800}{30} + \frac{1800}{72} + \frac{1800}{120} + \frac{1800}{90} - \frac{1800}{360} \\
&\quad = 1800 - 225 - 100 - 60 + 25 + 15 + 20 - 5 \\
&\quad = 1470.
\end{aligned}$$

Answer: 1470.

8. (a) We must show that $\preceq$ is reflexive, antisymmetric, and transitive. Since $a \leq a$ and $b \geq b$ for all $(a, b) \in P_n$, $\preceq$ is reflexive. It is antisymmetric since $(a_1, b_1) \preceq (a_2, b_2)$ and $(a_2, b_2) \preceq (a_1, b_1)$ is equivalent to $a_1 \leq a_2 \leq a_1$ and $b_1 \geq b_2 \geq b_1$, which indeed implies $(a_1, b_1) = (a_2, b_2)$. Finally, it is transitive because $(a_1, b_1) \preceq (a_2, b_2)$ and $(a_2, b_2) \preceq (a_3, b_3)$ means $a_1 \leq a_2 \leq a_3$ and $b_1 \geq b_2 \geq b_3$ which implies $a_1 \leq a_3$ and $b_1 \geq b_3$, i.e. $(a_1, b_1) \preceq (a_3, b_3)$. □

   (b) We move up in the Hasse diagram by either increasing the first component or decreasing the second. Hence, the diagram looks as follows: