LINKÖPINGS UNIVERSITET
Matematiska institutionen
Milagros Izquierdo

Tentamen i Diskret Matematik, TATA82, TEN1, 2017–08–17, kl 08–13.

Inga hjälpmedel. Ej räknedosa. Fullständiga motiveringar krävs.

För betyg 3 behövs 9 poäng, för betyg 4 12 poäng och 16 poäng för betyg 5.

---

1. Visa att $n! > n^3$ för alla $n \geq 6$.

2. (a) Visa att en graf med n^2 noder, alla med gradtal n, $n \geq 3$, inte kan vara planär.

   (b) Låt $K_{m,2}$ vara den fullständiga bipartita grafen med m noder av typ A och 2 noder av typ B. Visa att $K_{m,2}$ är planär.

   (c) Till en fest kommer 20 personer. Var och en hälsar på de festdeltagande som är bekanta (alla har någon bekant). Visa att det finns minst ett par av festdeltagare som har lika många bekanta.

3. Hur många positiva heltal mindre än 100.000 finns det om summan av dess siffror är mindre än eller lika med 20?

4. (a) Bestäm $103^{10547} mod 1260$. (2p)

   (b) I ett RSA-kryptosystem är den offentliga nyckeln $(323, 17)$, bestäm den associerade privata nyckeln (1p)

5. Lös den rekursiva ekvationen $a_{n+4} - 4a_{n+3} + 3a_{n+2} + 4a_{n+1} - 4a_n = (2)^{n+2}$, $n \geq 0, a_0 = 1, a_1 = 2, a_2 = 4, a_3 = 8$.

6. Betrakta meddelandet ESTETISK på alfabetet $\{E, S, T, I, K\}$. Betrakta prefixkoder $P = \{P(E),$
   $P(S), P(T), P(I), P(K)\}$ där varje P av en bokstav är en binär följd med någon längd och så att ingen P av bokstav är början på P av en annan bokstav. Kostnaden $c(P)$ för en prefixkod P är totallängden av $P(E)P(S)P(T)P(E)P(T)P(I)P(S)P(K)$. Vi definierar en relation $\mathcal{R}$ på prefixkoderna ovan som $P\mathcal{R}P'$ om $c(P) = c(P')$. Visa att relationen $\mathcal{R}$ är en ekvivalensrelation.

7. Visa att relationen $\mathcal{R}$ definierad i Uppgift 6 inte är en partialordning.

Written Examination in Discrete Mathematics TATA82, TEN1, 2017–08-17, kl 08–13.

No calculator.

For grade 3 are required 9 points, 12 points for grade 4 and 16 for grade 5.

Complete motivations required.

---

1. Show that $n! > n^3$ for all $n \geq 6$.

2. (a) Show that a graph with n^2 vertices, all of degree n, $n \geq 3$, is not planar.

   (b) Let $K_{m,2}$ be the complete bipartite graph with m vertices of type A and 2 vertices of type B. Show that $K_{m,2}$ is planar

   (c) 20 people come to a party. Each of them greets her/his acquaintances that are at the party (everyone has some acquaintance at the party). Show that there are two people at the party with the same number of acquaintances at the party.

3. How many positive integers smaller than 100.000 are there if the sum of the digits is smaller or equal to 20?

4. (a) Determine $103^{10547} mod 1260$. (2p)

   (b) In one RSA cryptographic system the public key is $(323, 17)$, determine the private key (1p)

5. Solve the recursive equation $a_{n+4} - 4a_{n+3} + 3a_{n+2} + 4a_{n+1} - 4a_n = (2)^{n+2}$, $n \geq 0, a_0 = 1, a_1 = 2, a_2 = 4, a_3 = 8$.

6. Consider the message ESTETISK on the alphabet $\{E, S, T, I, K\}$. Consider prefixcodes $P = \{P(E), P(S), P(T), P(I), P(K)\}$ where each P of a letter is a binary sequence of some length so that no P of a letter is the start of P of another letter. The cost $c(P)$ for a prefixcode P is the total length of $P(E)P(S)P(T)P(E)P(T)P(I)P(S)P(K)$. We define a relation $\mathcal{R}$ on the prefixcodes above by $P\mathcal{R}P'$ if $c(P) = c(P')$. Show that $\mathcal{R}$ is an equivalence relation.

7. Show that the relation $\mathcal{R}$ defined in Exercise 6 is not a partial order.

Svar Discrete Mathematics TATA52/ÅE2 17/8 2017

1) Show that $n! > n^3$ for all $n \geq 8$

With Math. Induction, first show that

for $n = 6$ $\quad 6! = 720 > 216 = 6^3$ .OK

ii) Assume that $p! > p^3$ for $p \geq 6$ and show that $(p+1)! > (p+1)^3$. But

$(p+1)! = (p+1)\,p! > (p+1)\cdot p^3$ and $p^3 > (p+1)^2$

$p^3 > (p+1)^2 + 1 \Leftrightarrow p^2(p-1) - 2(p+1) > 0$ $\quad \begin{matrix} p^2 > p+1, & p \geq 6 \\ p-1 > 2, & p \geq 6 \end{matrix}$ for $p \geq 6$

So $(p+1)! > (p+1)^3$ for $p \geq 6$. As required.

2) a) Let G be a graph with $v = n^2$ vertices and e edges

$2e = n^3$, $n \geq 3$, $e = \frac{n^3}{2} \geq 3n^2 - 6$ i.e. $n^3 \geq 6n^2 - 12$ for $n \geq 3$

then G cannot be planar

b) $K_{m,2}$ cannot contain K_5 or $K_{3,3}$

c) By pigeonhole principle: each of the participants at the party can have between 1 and 19 acquaintances but $20 = 19 + 1$.

3) Consider number $n = d_1 d_2 d_3 d_4 d_5$ s.t $d_1 + d_2 + d_3 + d_4 + d_5 \leq 20$ and $9 \geq d_i \geq 0$. This is equivalent to the number of solutions of the equation

$$d_1 + d_2 + d_3 + d_4 + d_5 + s = 20, \quad s \geq 0, \quad 0 \leq d_i \leq 9$$

Consider the sets $A_i = \{$solutions, where $d_i \geq 10\}$, $1 \leq i \leq 5$

We look for $|\mathcal{U}| - |A_1 \cup A_2 \cup A_3 \cup A_4 \cup A_5|$, with

$|\mathcal{U}| = \binom{25}{5}$, $|A_i| = \binom{15}{5}$, $|A_i \cap A_j| = \binom{5}{5} = 1$, $\forall i, j$

$|A_{i_1} \cap A_{i_2} \cap A_{i_3}| = 0 = |A_{i_1} \cap A_{i_2} \cap A_{i_3} \cap A_{i_4}| = |A_1 \cap A_2 \cap A_3 \cap A_4 \cap A_5|$

So the number of integers is $\binom{25}{5} - 5\binom{15}{5} + 10 = 2320$ integers

4)a) $103^{10547} \bmod 1260$. With Chinese Remainder Th.

$N = 1260 = 9 \times 7 \times 4 \times 5$

$103^{10547} \equiv 4^5 \equiv 7 \bmod 9$, $103^{10547} \equiv 5^5 \equiv 3 \bmod 7$

$103^{10547} \equiv 2 \bmod 5$, $103^{10547} \equiv 3 \bmod 4$

$103^{10547} \equiv (7 \times 140 x_1 + 3 \times 180 x_2 + 2 \times 252 x_3 + 3 \times 315 x_4) \bmod 1260$

$140x_1 \equiv 1 \bmod 9$	$180x_2 \equiv 1 \bmod 7$	$252x_3 \equiv 1 \bmod 5$	$315x_4 \equiv 1 \bmod 4$
$5x_1 \equiv 1 \bmod 9$	$5x_2 \equiv 1 \bmod 7$	$2x_3 \equiv 1 \bmod 5$	$-x_4 \equiv 1 \bmod 4$
$x_1 \equiv 2$	$x_2 \equiv 3$	$x_3 \equiv 3$	$x_4 \equiv -1 \bmod 4$

so $103^{10547} \equiv (1960 - 1620 + 1512 - 945) \bmod 1260 \equiv \underline{907}$

b) Public key $(N, 4) = (323, 17)$ $N = 323 = 19 \times 17$

$\phi(N) = 18 \times 16 = 288$. Private key a satisfies

$17a \equiv 1 \bmod 288$, $\underline{a = 17}$ $(17^2 = 289)$

5) Solve $a_{n+4} - 8a_{n+3} + 3a_{n+2} + 4a_{n+1} - 4a_n = (2)^{n+2}$

$a_0 = 1$, $a_1 = 2$, $a_2 = 4$, $a_3 = 8$

Homegeneous eq. with characteristic eq $r^4 - 4r^3 + 3r^2 + 4r - 4 = 0$

and roots $r_1 = 2$, $m_1 = 2$; $r_2 = 1$, $m_2 = 1$; $r_3 = -1$, $m_3 = 1$

$a_n^{(h)} = (2)^n (A_1 + A_2 n) + A_3 + (-1)^n A_4$

Particular solution $a_n^{(p)} = B(2)^n n^2$, where

$16B(2)^n(n+4)^2 - 32B(2)^n(n+3)^2 + 12B(2)^n(n+2)^2 + 8B(2)^n(n+1)^2 - 4B(2)^n n^2$

$n^2(16B - 32B + 12B + 8B - 4B) + n(128B - 192B + 48B + 16B) +$

$+ 256B - 288B + 48B + 8B = 4$

$\begin{cases} 0 = 0 & (n^2) \\ 0 = 0 & (n) \\ 24B = 4, & \end{cases}$ $\overset{11}{4}(2)^n$

$\underline{B = 1/6}$, $a_n = (2)^n \left(A_1 + A_2 n + \frac{n^2}{6}\right) + A_3 + (-1)^n A_4$

IC $\begin{cases} a_0 = 1 = A_1 + A_3 + A_4 \\ a_1 = 2 = 2A_1 + 2A_2 + A_3 - A_4 + 1/3 \\ a_2 = 4 = 4A_1 + 8A_2 + A_3 + A_4 + 8/3 \\ a_3 = 8 = 8A_1 + 24A_2 + A_3 - A_4 + 12 \end{cases}$

$A_1 = -\frac{79}{9}$

$A_2 = 10/3$

$A_3 = 67/6$

$A_4 = -25/18$

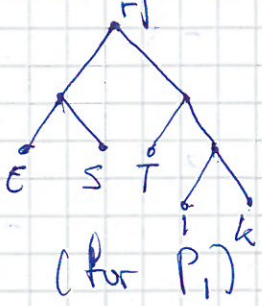
$a_n = (2)^n \left(\frac{n^2}{6} + \frac{10n}{3} - \frac{79}{9}\right) + \frac{67}{6} + (-1)^n \frac{25}{18}$

6) $\mathcal{P} = \{P$, prefixcode on E, S, T, I and $4\}$
We define a relation by $P \mathcal{R} P'$ if $c(P) = c(P')$
$c(P)$ = total length of the binary sequence
$P(E)P(S)P(T)P(E)P(T)P(I)P(S)P(4)$ for any code P
i) $\mathcal{R}$ is reflexive since for every prefixcode P
$c(P) = c(P)$
ii) $\mathcal{R}$ is symmetric since if $c(P) = c(P')$ i.e
$P \mathcal{R} P'$, also $c(P') = c(P)$ and $P' \mathcal{R} P$
iii) $\mathcal{R}$ is transitive since if $P \mathcal{R} P'$ and $P' \mathcal{R} P''$
we have $c(P) = c(P')$ and $c(P') = c(P'')$, then
$c(P) = c(P'')$ and $P \mathcal{R} P''$ as wanted.
So $\mathcal{R}$ is an equivalence relation.

Exercise 7 is only for TATA82

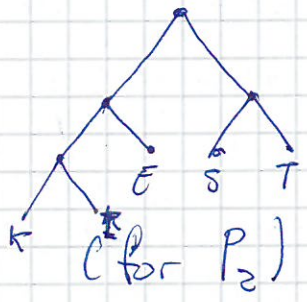
$\mathcal{R}$ is not a partial order since the codes
$P_1 = \{P_1(E)=00,\ P_1(S)=01,\ P_1(T)=10,\ P_1(I)=110,\ P_1(4)=111\}$
and $P_2 = \{P_2(E)=01,\ P_2(S)=10,\ P_2(T)=11,\ P_2(I)=001,\ P_2(4)=000\}$
have $c(P_1) = c(P_2)$ so $P_1 \mathcal{R} P_2$ and $P_2 \mathcal{R} P_1$
but $P_1 \neq P_2$

The corresponding binary rooted trees are



(for P_1)

and



(for P_2)

LINKÖPINGS UNIVERSITET
Matematiska institutionen
Milagros Izquierdo

Tentamen i Diskret Matematik, TATA52, TEN1, 2016–08–17, kl 8–13.

Inga hjälpmedel. Ej räknedosa. Fullständiga motiveringar krävs.

För betyg N behövs 3N-1 poäng.

---

1. Visa att $n! > n^3$ för alla $n \geq 6$.

2. (a) Visa att en graf med n^2 noder, alla med gradtal n, $n \geq 3$, inte kan vara planär.

   (b) Låt $K_{m,2}$ vara den fullständiga bipartita grafen med m noder av typ A och 2 noder av typ B. Visa att $K_{m,2}$ är planär.

   (c) Till en fest kommer 20 personer. Var och en hälsar på de festdeltagande som är bekanta (alla har någon bekant). Visa att det finns minst ett par av festdeltagare som har lika många bekanta.

3. Hur många positiva heltal mindre än 100.000 finns det om summan av dess siffror är mindre än eller lika med 20?

4. (a) Bestäm $103^{10547} mod 1260$. (2p)

   (b) I ett RSA-kryptosystem är den offentliga nyckeln $(323, 17)$, bestäm den associerade privata nyckeln (1p)

5. Lös den rekursiva ekvationen $a_{n+4} - 4a_{n+3} + 3a_{n+2} + 4a_{n+1} - 4a_n = (2)^{n+2}$, $n \geq 0, a_0 = 1, a_1 = 2, a_2 = 4, a_3 = 8$.

6. Betrakta meddelandet ESTETISK på alfabetet $\{E, S, T, I, K\}$. Betrakta prefixkoder $P = \{P(E), P(S), P(T), P(I), P(K)\}$ där varje P av en bokstav är en binär följd med någon längd och så att ingen P av bokstav är början på P av en annan bokstav. Kostnaden $c(P)$ för en prefixkod P är totallängden av $P(E)P(S)P(T)P(E)P(T)P(I)P(S)P(K)$. Vi definierar en relation $\mathcal{R}$ på prefixkoderna ovan som $P\mathcal{R}P'$ om $c(P) = c(P')$. Visa att relationen $\mathcal{R}$ är en ekvivalensrelation.