Aalto-universitetet

Gripenberg

MS-A0409 Grundkurs i diskret matematik
Mellanförhör 2, 23.10.2014

Skriv ditt namn, nummer och övriga uppgifter på varje papper!
Räknare eller tabeller får **inte** *användas i detta prov!*

1. (4p) Använd Euklides algoritm för att bestämma den största gemensamma delaren av talen 85 och 55.
Lösning: I enlighet med Euklides algoritm räknar vi ut r_j, $j \geq 0$ så att $r_{j-2} = q_j r_{j-1} + r_j$ då $j \geq 0$ och $0 \leq r_j < r_{j-1}$ med $r_0 = 85$ och $r_1 = 55$ och vi får

$$\begin{aligned} 85 &= 1 \cdot 55 + 30 \\ 55 &= 1 \cdot 30 + 25 \\ 30 &= 1 \cdot 25 + 5 \\ 25 &= 5 \cdot 5 + 0 \end{aligned}$$

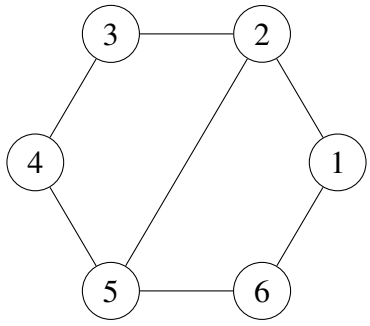
Av detta ser vi att den största gemensamma delaren är 5.

---

2. (4p) För att kryptera ett meddelande med RSA-algoritmen användes den publika nyckeln $(77, 17)$. Är den privat nyckeln då $(77, 3)$? Motivera ditt svar!
Lösning: Eftersom $n = 77 = 7 \cdot 11$ så skall vi räkna ut $m = (7-1) \cdot (11-1) = 60$. Den privata nyckeln (n, d) bestäms så att $[d]_m = [k]_m^{-1}$ då den publika nyckeln är (n, k). Detta innebär att mod $(d \cdot k, m) = 1$ så att om den privata nyckeln skulle vara $(77, 3)$ så borde mod $(3 \cdot 17, 60) =$ mod $(51, 60) = 51$ vara 1 så vi ser att $(77, 3)$ inte kan vara den privata nyckeln.

---

3. (6p) Bestäm alla permutationer ψ av noderna i grafen $[V, E]$ nedan som är grafisomorfismer, dvs. är sådana att om det finns en båge mellan noderna a och b så finns det en båge mellan noderna $\psi(a)$ och $\psi(b)$. Uttryck permutationerna med cykelnotation. Dessa permutationer bildar en grupp G (med det behöver du inte visa). Bestäm cykelindexet $\zeta_{G,V}$. Vad kan detta index användas till?



Lösning: Permutationerna är (1) (identitetsfunktionen), $(1\ \ 4)(2\ \ 5)(3\ \ 6)$ (rotation $180°$), $(1\ 6)(2\ 5)(3\ 4)$ (en spegling) och $(1\ 3)(4\ 6)$ (en annan spegling) där cyklar med längden 1 inte skrivits ut. Cykelindexet blir därför

$$\zeta_{G,V}(t_1, t_2) = \frac{1}{4}\big(t_1^6 + t_1^2 t_2^2 + 2t_2^3\big).$$

Cykelindexet kan användas för att svara på vissa frågor beträffande antal ”färgningar” som inte är ekvivalenta under verkan av gruppen G. Om man tex. i_j gånger använder färgen a_j, $j = 1, \ldots, r$ så är koefficienten för $a_1^{i_1} \cdot a_2^{i_2} \cdot \ldots \cdot a_r^{i_r}$ i $\zeta_{G,V}(a_1 + \ldots + a_r, a_1^2 + \ldots + a_r^2, \ldots, a_1^n + \ldots + a_r^n)$ antalet icke-ekvivalenta färgningar och $\zeta_{G,V}(r, \ldots, r)$ är antalet färgningar med r färger.

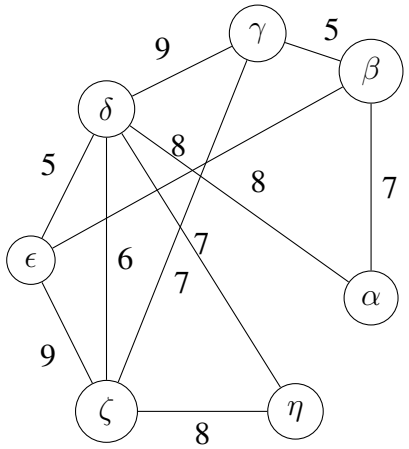
---

4. (4p) Antag att i en icke-riktad, enkel (dvs. ingen båge från någon nod till sig själv) och sammanhängande graf finns 4 noder som alla har 3 grannar var och resten har alla 4 grannar. Är det möjligt att hitta en Euler-väg i grafen, dvs. en väg som går genom alla bågar exakt en gång.

Lösning: Antag att $[v_0, v_1, \ldots, v_n]$ är en sådan väg. För varje index $j \in \{1, 2, \ldots, n-1\}$ gäller att v_{j-1} och v_{j+1} är grannar till v_j och det kan inte vara så att $v_{j-1} = v_{j+1}$ för då skulle vägen gå genom bågen $\{v_{j-1}, v_j\}$ två gånger. Eftersom vägen går genom alla bågar kan vi räkna antalet grannar till en nod v så att vi för varje gång v förekommer bland noderna v_j med $j \in \{1, 2, \ldots, n-1\}$ ökar vi antalet grannar med två och om $v = v_0$ eller $v = v_n$ ökar vi antalet grannar med 1. Dethär innebär att det bara är noderna v_0 och v_n som kan ha ett udda antal grannar (och om $v_0 = v_n$ så har också denhär noden ett jämnt antal grannar). Därför kan det inte finnas en Euler-väg i en graf där det finns exakt 4 noder med ett udda antal grannar.

---

5. (6p) Bestäm ett minimalt uppspännande träd för grafen nedan genom att använda en algoritm som garanterat ger ett optimalt resultat (men du skall inte visa att algoritmen ger ett optimalt resultat). Förklara hur du gått tillväga tex. genom att skriva ner i vilken ordning du lagt bågar trädet.



Vikterna för bågarna är följande:

$$w(\{\alpha, \beta\}) = 7, \quad w(\{\beta, \gamma\}) = 5, \quad w(\{\gamma, \delta\}) = 9, \quad w(\{\delta, \epsilon\}) = 5,$$
$$w(\{\epsilon, \zeta\}) = 9, \quad w(\{\zeta, \eta\}) = 8, \quad w(\{\alpha, \delta\}) = 8, \quad w(\{\beta, \epsilon\}) = 8,$$
$$w(\{\gamma, \zeta\}) = 7, \quad w(\{\delta, \zeta\}) = 6, \quad w(\{\delta, \eta\}) = 7.$$

Lösning: Om vi använder den giriga algoritm (Prims) som startar med en godtycklig nod och sedan lägger till en nod och en båge mellan det träd som redan konstruerats och den nya noden

så att vikten av denna båge är så liten som möjligt och om vi som första nod i trädet väljer α så blir delträden följande:

$[\{\alpha\}, \emptyset]$,
$[\{\alpha, \beta\}, \{\{\alpha, \beta\}\}]$,
$[\{\alpha, \beta, \gamma\}, \{\{\alpha, \beta\}, \{\beta, \gamma\}\}]$,
$[\{\alpha, \beta, \gamma, \zeta\}, \{\{\alpha, \beta\}, \{\beta, \gamma\}, \{\gamma, \zeta\}\}]$,
$[\{\alpha, \beta, \gamma, \zeta, \delta\}, \{\{\alpha, \beta\}, \{\beta, \gamma\}, \{\gamma, \zeta\}, \{\zeta, \delta\}\}]$,
$[\{\alpha, \beta, \gamma, \zeta, \delta, \epsilon\}, \{\{\alpha, \beta\}, \{\beta, \gamma\}, \{\gamma, \zeta\}, \{\zeta, \delta\}, \{\delta, \epsilon\}\}]$,
$[\{\alpha, \beta, \gamma, \zeta, \delta, \epsilon, \eta\}, \{\{\alpha, \beta\}, \{\beta, \gamma\}, \{\gamma, \zeta\}, \{\zeta, \delta\}, \{\delta, \epsilon\}, \{\delta, \eta\}\}]$.

Om vi använder den giriga algoritm som väljer den båge som har minst vikt så att delgrafen förblir en skog (Kruskals algoritm) får vi tex. följande delgrafer:

$[\{\beta, \gamma\}, \{\{\beta, \gamma\}\}]$,
$[\{\beta, \gamma, \delta, \epsilon\}, \{\{\beta, \gamma\}, \{\delta, \epsilon\}\}]$,
$[\{\beta, \gamma, \delta, \epsilon, \eta\}, \{\{\beta, \gamma\}, \{\delta, \epsilon\}, \{\delta, \eta\}\}]$,
$[\{\beta, \gamma, \delta, \epsilon, \zeta, \eta\}, \{\{\beta, \gamma\}, \{\delta, \epsilon\}, \{\delta, \eta\}, \{\delta, \zeta\}\}]$,
$[\{\alpha, \beta, \gamma, \delta, \epsilon, \zeta, \eta\}, \{\{\beta, \gamma\}, \{\delta, \epsilon\}, \{\delta, \eta\}, \{\delta, \zeta\}, \{\alpha, \beta\}\}]$,
$[\{\alpha, \beta, \gamma, \delta, \epsilon, \zeta, \eta\}, \{\{\beta, \gamma\}, \{\delta, \epsilon\}, \{\delta, \eta\}, \{\delta, \zeta\}, \{\alpha, \beta\}, \{\gamma, \zeta\}\}]$.
