Aalto-universitetet

Gripenberg

MS-A0409 Grundkurs i diskret matematik
Mellanförhör 2, 24.10.2013

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

1. (6p) Använd Euklides algoritm (även om det kanske vore lika enkelt att resonera på något annat sätt) för att bestämma den största gemensamma delaren till talen 126 och 48. Förklara hur man med hjälp av detta resultat kan avgöra om det finns heltalslösningar till ekvationen $2 = 126x + 48y$. (I det fall att det finns lösningar är det inte nödvändigt att bestämma dem, det räcker med att förklara varför de finns.)

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 $r_0 = 126$ och $r_1 = 48$ och vi får

$$\begin{aligned} 126 &= 2 \cdot 48 + 30 \\ 48 &= 1 \cdot 30 + 18 \\ 30 &= 1 \cdot 18 + 12 \\ 18 &= 1 \cdot 12 + 6 \\ 12 &= 2 \cdot 6 + 0 \end{aligned}$$

Av detta ser vi att den största gemensamma delaren är 6.

Om det skulle finnas heltal x och y så att $2 = 126x + 48y$ så skulle vi se att 6 delar 2 eftersom 6 delar både 126 och 48. Eftersom 6 inte delar 2 så kan det inte finnas sådana heltal x och y.

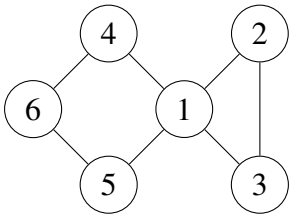
---

2. (4p) En person som ville använda RSA-algoritmen för kryptering bestämde en publik och en privat nyckel för detta ändamål men glömde sedan (innan hen hade publicerat den publika nyckeln) vilken som var vilken. Spelar detta någon roll? Motivera ditt svar.

Lösning: De publika och privata nycklarna (n, k) och (n, d) i RSA-algoritmen väljs så att $[k]_m \cdot [d]_m = [1]_m$ där $m = (p-1) \cdot (q-1)$ då $n = p \cdot q$. Eftersom $[k]_m \cdot [d]_m = [d]_m \cdot [k]_m$ är de publika och privata nycklarna helt symmetriska och det spelar ingen roll vilken som väljs att publiceras.

---

3. (6p) Bestäm alla permutationer f 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 $f(a)$ och $f(b)$. 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?



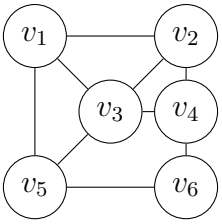
Lösning: Permutationerna är (1), $(2\ 3)$, $(4\ 5)$ och $(2\ 3)(4\ 5)$ (där cyklar med längden 1 inte skrivits ut). Cykelindexet blir därför

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

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-ekvivalenmta färgningar och $\zeta_{G,V}(r, \ldots, r)$ är antalet färgningar med r färger.

---

4. (4p) I grafen nedan har noderna v_j, $j = 1, 2, \ldots, 6$ ”färgats” med färgerna a, b och c så att $\omega(v_1) = b$, $\omega(v_2) = c$, $\omega(v_3) = a$, $\omega(v_4) = b$, $\omega(v_5) = c$ och $\omega(v_6) = a$. Sätt noderna i en ordning så att den giriga nodfärgningsalgoritmen ger denna färgning (då färgerna är i alfabetisk ordning). Varför är det inte möjligt att färga noderna med två färger så att noder mellan vilka det finns en båge får olika färger?



Lösning: En möjlig ordning är

$$v_6, \quad v_3, \quad v_4, \quad v_1, \quad v_5, \quad v_2$$

Eftersom tex. noderna v_1, v_2 och v_3 alla är grannar med varandra kan de inte (och därför inte hela grafen heller) färgas med två färger så att noder mellan vilka det inte finns en båge får olika färger.

---

5. (4p) Ett träd är som bekant en enkel graf i vilken det finns exakt en enkel väg från varje nod till varje annan nod. Antag att G är ett träd med $n \geq 3$ noder så att det finns en Hamilton väg i G (dvs. en enkel väg som går genom alla noder). En hurudan graf är G? Motivera ditt svar!

Lösning: Antag att grafen är $[V, E]$ och att $[v_0, v_1, \ldots, v_n]$ är Hamiltonvägen, dvs $|V| = n + 1$, $v_j \neq v_k$ då $0 \leq j < k \leq n$ och $\{v_{j-1}, v_j\} \in E$ då $j = 1, 2, \ldots, n$. Om det nu finns någon annan båge i E än $\{v_{j-1}, v_j\}$, tex. $\{v_p, v_q\}$ med $p \leq q - 2$ så är $[v_0, \ldots, v_p, v_q, \ldots, v_n]$ an annan enkel väg från v_0 till v_n och en sådan kan inte finnas eftersom grafen är ett träd. Detta innebär att grafen ser ut på följande sätt: