KTH, 20040414
Tentamen i Diskret matematik 5B1118, IT1
Skrivtid: 14.00-19.00

Inga hjälpmedel. Skriv prydligt. Motivera lösningarna väl. Betygsgränser: 20p för 3, 24p för 4, 28p för 5. Lycka till!

DEL A, 3p per uppgift

1. Visa med induktion att om $a_0 = 0$ och $a_n = 2a_{n-1} + 1$ så är $a_n = 2^n - 1$.
   Lösning: (**induktionsbas**) $a_0 = 0 = 2^0 - 1$
   (**induktionshypotes**) $a_p = 2^p - 1$
   (**induktionsövergång**) $a_{p+1} = 2\,a_p + 1 = 2(2^p - 1) + 1 = 2^{p+1} - 1$ VSV.

2. Hitta alla positiva heltalslösningar till ekvationen $5x + 7y = 120$.
   Lösning: Lätt att inse att $x = y = 10$ är en partikulär lösning. Den allmäna lösningen är då
   $x = 10 + 7n$, $y = 10 - 5n$, n ett godtyckligt heltal.
   För att x och y blir positiva måste $n \leq 10/5$ och $n \geq -10/7$ dvs $n = -1, 0, 1, 2$. Detta ger
   Följande lösningar: $(x, y) = (3, 15), (10, 10), (17,5)$ och $(24, 0)$.

3. Hur många olika ord med 6 bokstäver kan man bilda med bokstäverna i ordet KOMBINATORIK?
   Lösning: vi har 2 av K, I och O. Så det bara kan förekomma dubletter.
   - **Inga dubletter**. Då finns det 9 olika bokstäver att fördela på 6 platser på 9_8_7_6_5_4 sätt.
   - **En dublett**. 3 sätt att välja vilken (KK, II eller OO) _ $\binom{6}{2}$ sätt att välja var den ska stå _ 8 resterande bokstäver på 4 resterande platser = 3_$\binom{6}{2}$_8_7_6_5 sätt
   - **Två dubletter.** 3_$\binom{6}{2}$ sätt att placera den första _ 2_$\binom{4}{2}$ sätt att placera den andra _ 7_6 sätt att placera bokstäver som är kvar på 2 platser som är kvar = 3_$\binom{6}{2}$_2_$\binom{4}{2}$ _7_6 sätt
   - **Tre dubletter.** $\binom{6}{2}$ sätt att placera K _ $\binom{4}{2}$ sätt att placera I (O placeras på de resterande två platser)

   SVAR: 9_8_7_6_5_4 + 3_$\binom{6}{2}$_8_7_6_5 + 3_$\binom{6}{2}$_2_$\binom{4}{2}$ _7_6 + $\binom{6}{2}$ _ $\binom{4}{2}$ sätt.

4. Den publika (allmäna) nyckeln för ett RSA-schema är (n = 187, e = 107). Bestäm dekrypteringsexponenten d och dekryptera meddelandet ”100”.
   Lösning: n = 11_17, alltså blir ed _ 1 (mod 10_16). Detta ger
   $107d + 160m = 1$,
   vilken är en Diofantisk ekvation. Löser man den, hittar man att $d = 3$.
   $100^3 = 1000000 = 187\_5347 + 111$, så den dekrypterade meddelanden är ”111”.

5. Beräkna $aba^{-1}b^{-1}$ för följande permutationer

   a) a = (12), b = (345). SVAR: id = (1)(2)(3)(4)(5)
   b) a = (12), b = (245). SVAR: (142)

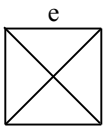
6. Avgör om grafen med incidenstabellen

1	2	3	4	5	6
2	1	2	1	1	1
4	3	4	3	2	2
5	5	5	5	3	3
6	6	6	6	4	4

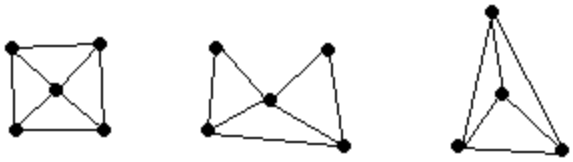
har en Hamilton-stig. Har den en Eulersk stig också?
Lösning: Eulersk cykel : 1-2-6-1-5-2-3-5-4-3-6-4-1
Hamiltonsk cykel: 1-5-2-6-3-4-1

DEL B, 4p per uppgift

7. Beräkna kromatiska polynomet för grafen (varje skärningspunkt räknas som ett av grafens hörn)

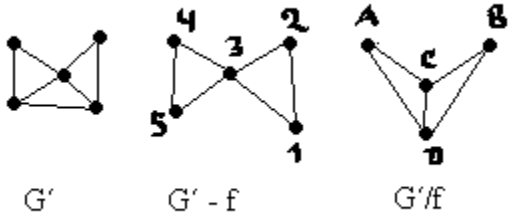


Lösning: Kalla våran graf G. Dess kromatiska polynom är $P(G, x)$.Vi använder oss av satsen som säger att $P(G, x) = P(G - e, x) - P(G/e, x)$.



G/e är den kompletta grafen K_4 med kromatiska polynomet $x(x-1)(x-2)(x-3)$.

När det gäller G´ = G – e, upprepar vi samma procedur:



För att färga G´– f börjar vi med hörnet 1 (x sätt) och sedan 2 ($x-1$ sätt), 3 ($x-2$ sätt), 4 ($x-1$ sätt) och 5 ($x-2$ sätt).

$$P(G´- f, x) = x(x-1)(x-2)(x-1)(x-2).$$

Färgning av G´/f görs genom att färga A och B samma (x sätt), C ($x-1$ sätt) och D ($x-2$ sätt) eller genom att färga de olika ($x(x-1)$ sätt), C ($x-2$ sätt) och D ($x-3$ sätt).

$$P(G´/f, x) = x(x-1)(x-2) + x(x-1)(x-2)(x-3).$$

Svaret blir således:

$$P(G, x) = x(x-1)(x-2)(x-1)(x-2) - [x(x-1)(x-2) + x(x-1)(x-2)(x-3)] - x(x-1)(x-2)(x-3) =$$
$$= x(x-1)(x-2)[x^2 - 5x + 7].$$

8. Beskriv krypteringsmetoden med en allmänn nyckel. Förklara även hur en digital signatur kan skapas med hjälp av metoden.

   Lösning: Alice har 2 stycken krypteringsnycklar, en publik och en hemlig. Bob krypterar sitt meddelande till Alice med hennes allmänna nyckel. Det är bara Alice som kan dekryptera meddelandet med sin hemliga nyckel.
   Underskriften kan skapas t ex genom att Bob krypterar först sin egen hemliga nyckel, skriver under ”Bob” och krypterar alltsammans med Alices allmänna nyckel.
   Alice dekrypterar meddelandet med sin hemliga nyckel och ser Bobs underskrift.
   Med hjälp av Bobs almänna nyckel dekrypterar hon resultatet och får det ursprungliga meddelandet.

9. Förklara varför två permutationer med samma cykeltyp är alltid konjugerade.
   Lösning: se lösningen till övning 5.15 i anteckningar till föreläsning 15.

10. Låt G vara en mängd av element $\{ \mathbf{0}_x, \mathbf{1}_y \mid x, y \text{ i } \mathbf{Z}_5 \}$. Operationen * definieras som

$$\mathbf{0}_x * \mathbf{0}_y = \mathbf{0}_{x+y};\ \mathbf{1}_x * \mathbf{0}_y = \mathbf{1}_{x-y};\ \mathbf{0}_x * \mathbf{1}_y = \mathbf{1}_{x+y} \text{ och } \mathbf{1}_x * \mathbf{1}_y = \mathbf{0}_{x-y}.$$

    Visa att (G, *) är en grupp med 10 element. Bestäm ordningen av alla element i G.

    Lösning: Direkt kontroll visar att * är associativ.
    identiteten är $\mathbf{0}_0$.
    Inversen till $\mathbf{0}_y$ är $\mathbf{0}_{-y}$.
    $\mathbf{1}_y$ är sin egen invers och har då ordning 2.
    $\mathbf{0}_y$ kommuterar med övriga element och har ordning 5.