**KTH Matematik**
B.Ek

**Lösningar tentamen 5B1204 Diskret matematik för D2, 9 mars 2005**

## Teoridel

**1a)** Karakteristiska ekvationen till den sökta rekursionsekvationen har enkelrötterna $x = 7, -2$, så den är $(x-7)(x+2) = 0$, dvs $x^2 - 5x - 14 = 0$ och den sökta ekvationen: $a_{n+2} = 5a_{n+1} + 14a_n$. Se stencilen om rekursionsekvationer.
**b)** Se Biggs 15.3. **c)** Se Biggs 15.5.
**2a)** Se Biggs 17.3. **b)** $v - e + r - c = 1$. Se stencilen om plana och planära grafer.
**c)** Se Biggs 17.4. Villkoret är nödvändigt och tillräckligt.
**3a)** Se Biggs 5.2.
**b)** Oordnat val (identiska kulor) av $r$ st med upprepning (gott om plats i lådorna) bland $n$ st, så på $\binom{n+r-1}{r} = \binom{n+r-1}{n-1}$ sätt, se Biggs 11.2.
**c)** Se Biggs 12.6. $\pi = (1\,4\,2\,7)(3\,6)(5)$, så $\pi$ är en **jämn** permutation (ett jämnt antal udda cykler (dvs cykler av jämn längd)).
**4a)** Se Biggs 10.3 **b), c)** Se Biggs 13.3.
**5a)** Nej, $|S_m \times S_n| = |S_m||S_n| = m!n! < (m+n)! = |S_{m+n}|$ (om $m, n > 0$), så det finns ingen bijektion $S_m \times S_n \to S_{m+n}$. ($S_m \times S_n$ är (isomorf med) gruppen av permutationer av kopior av $\mathbb{N}_m$ och $\mathbb{N}_n$, var för sig.) Se Biggs 20.5,6.
**b)** $G$:s ordning är en multipel av elementets ordning (Biggs 20.8), så bara 30 och 105 är tänkbara. Exemplen $C_{30}$ och $C_{105}$ visar att de också är möjliga. Se även Biggs 20.9.
**c)** Se Biggs 20.8.

## Problemdel

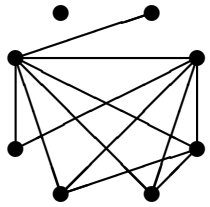
**6a)** $n = 703 = 19 \cdot 37$, så $m = (19-1)(37-1) = 18 \cdot 36 = 648$. $e = 77$, så $d$ skall uppfylla $77d \equiv_{648} 1$. Använd Euklides algoritm: $648 = 8 \cdot 77 + 32$, $77 = 2 \cdot 32 + 13$, $32 = 2 \cdot 13 + 6$, $13 = 2 \cdot 6 + 1$, så $1 = 13 - 2 \cdot 6 = 13 - 2(32 - 2 \cdot 13) = -2 \cdot 32 + 5 \cdot 13 = -2 \cdot 32 + 5(77 - 2 \cdot 32) = 5 \cdot 77 - 12 \cdot 32 = 5 \cdot 77 - 12(648 - 8 \cdot 77) = -12 \cdot 648 + 101 \cdot 77$ och vi kan ta $d = 101$, så **svar: en avkrypterinsnyckel är (703, 101).**
**b)** För att bestämma antalet kodord, löser vi systemet $Hx = 0$ med Gausselimination: $\begin{bmatrix} 1&0&1&1&0 \\ 0&1&1&1&0 \\ 1&1&0&1&1 \end{bmatrix} \overset{r1 \to r3}{\sim} \begin{bmatrix} 1&0&1&1&0 \\ 0&1&1&1&0 \\ 0&1&1&0&1 \end{bmatrix} \overset{r2 \to r3}{\sim} \begin{bmatrix} 1&0&1&1&0 \\ 0&1&1&1&0 \\ 0&0&0&1&1 \end{bmatrix}$. Två positioner (3 och 4) kan tydligen väljas godtyckligt, varvid systemet bestämmer positionerna 1, 2 och 5 entydigt. Det finns alltså $2^2$, dvs **4 kodord**. (Nämligen 00000, 11011, 11100, 00111.)
Om det mottagna ordet (som kolonnvektor) multipliceras med $H$ fås $H \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$, dvs $H$:s sista kolonn. Ett fel har alltså inträffat i sista positionen och **det sända ordet var 11011**.
**c)** Vi skall lösa ekvationen $x^2 \equiv x \pmod{703}$, dvs $x^2 - x = x(x-1) \equiv_{703} 0$. Eftersom $703 = 19 \cdot 37$ och 19 och 37 är relativt prima, är detta ekvivalent med $x(x-1) \equiv_{19} 0$ och $x(x-1) \equiv_{37} 0$. Eftersom 19 och 37 är primtal är alla lösningar till dessa ekvationer $x \equiv_{19} 0, 1$ respektive $x \equiv_{37} 0, 1$.
$x \equiv_{19} 0$ betyder att $x = 19t$ för något $t$ och $x \equiv_{37} 0, 1$ betyder då $19t \equiv_{37} 0, 1$, dvs $t \equiv_{37} 38t \equiv_{37} 0, 2$, så $t = 0, 2 + 37u, u \in \mathbb{Z}$ och $x = 19(0, 2 + 37u) = 0, 38 + 703u$, dvs $x \equiv_{703} 0, 38$. P.s.s. ger $x \equiv_{19} 1$ och $x \equiv_{37} 0, 1$ att $x \equiv_{703} -37, 1 \equiv_{703} 666, 1$.
Således: **Svar: Lösningar är alla $x$ som uppfyller en av** $x \equiv 0, 1, 38, 666 \pmod{703}$.

**7a)** Poängen på varje uppgift kan ta 3 värden (0, 1, 2), så enligt multiplikationsprincipen är antalet $3 \cdot 3 \ldots 3 = 3^{10}$ (= antalet funktioner från en 10-mängd (uppgifterna) till en 3-mängd (resultaten)). **Svar: $3^{10}$ (= 59049) olika fördelningar.**
**b)** Eftersom alla möjliga utfall skall antas minst en gång, är det sökta antalet = antalet surjektioner från en 10-mängd till en 3-mängd = $3!S(10, 3)$. Med "Stirlings triangel" (dvs rekursionsformeln för Stirlingtalen) fås $S(10, 3) = 9330$, så antalet är $6 \cdot 9330 = 55980$.
Alternativt kan man använda sållprincipen: Låt $X$ vara mängden av alla fördelningar (de i **a)**) och $A_0, A_1, A_2$ alla fördelningar **utan** 0, 1 resp, 2. Då är $|X| = 3^{10}$, $|A_i| = 2^{10}$, $|A_i \cap A_j| = 1^{10} = 1$, $|A_i \cap A_j \cap A_k| = 0$ (om $i, j, k$ alla olika) och det sökta antalet $|X \setminus (A_0 \cup A_1 \cup A_2)| = |X| - (|A_0| + |A_1| + |A_2|) + (|A_0 \cap A_1| + |A_1 \cap A_2| + |A_2 \cap A_0|) - |A_0 \cap A_1 \cap A_2| = 3^{10} - 3 \cdot 2^{10} + 3 \cdot 1^{10} - 1 \cdot 0^{10} = 59049 - 3072 + 3 - 0 = 55980$.
**Svar: 55980 olika fördelningar.**

**7c)** Vi använder sållprincipen. Låt som nyss $X$ vara alla fördelningar och $B_0, B_1, B_2$ alla fördelningar med 0, 1 resp. 2 **högst en gång**. Då är $|B_i| = 2^{10} + 10 \cdot 2^9 = 6144$ (de utan $i$ + de med exakt ett $i$), $|B_i \cap B_j| = 1+10+10+10 \cdot 9 = 111$ (om $i \neq j$) (de utan $i, j$ + de med ett $i$, inget $j$ + de utan $i$, ett $j$ + de med ett $i$, ett $j$) och $|B_i \cap B_j \cap B_k| = 0$ (om $i, j, k$ alla olika) (inga med högst ett vardera av 0, 1, 2). Så det sökta antalet: $|X \setminus (B_0 \cup B_1 \cup B_2)| = |X| - (|B_0| + |B_1| + |B_2|) + (|B_0 \cap B_1| + |B_1 \cap B_2| + |B_2 \cap B_0|) - |B_0 \cap B_1 \cap B_2| = 59049 - 3 \cdot 6144 + 3 \cdot 111 - 1 \cdot 0 = 59049 - 18432 + 333 - 0 = 40950$.
**Svar: 40950 olika fördelningar.**

**8a)** $x \equiv 1 \pmod{12}$ betyder att $x = 1 + 12t$ för något $t \in \mathbb{Z}$. Villkoret $x \equiv 6 \pmod{13}$ ger $1 + 12t \equiv_{13} 6$, dvs $-t \equiv_{13} 12t \equiv_{13} 5$, så $t \equiv_{13} -5 \equiv_{13} 8$ och alla lösningar blir $x = 1 + 12(8 + 13u) = 97 + 156u$, $u \in \mathbb{Z}$ godtyckligt. (Man kan förstås också göra som i stencilen om kinesiska restsatsen.) **Svar: Alla $x$ som uppfyller $x \equiv 97 \pmod{156}$.**
**b)** Vi vet att (med $P_n = \{p; p \text{ primtal}, p \mid n\}$) $\phi(n) = n \prod_{p \in P_n} (1 - \frac{1}{p})$. Så om $\phi(n) = 10$ och $p$ är en primfaktor i $n$, måste $(p-1) \mid 10$, dvs $p - 1 = 1, 2, 5$ eller 10. $n$ innehåller tydligen inga andra primfaktorer än 2, 3, 11. Om inte 11 ingår i $n$ kommer inte faktorn 5 med, så $11 \mid n$ och övriga faktorer skall ge 1, så **svar: $n$ är 11 eller 22**.
**c)** $1193^n \equiv 1 \pmod{861}$ är ekvivalent med att $1193^n \equiv_3 1$, $1193^n \equiv_7 1$ och $1193^n \equiv_{41} 1$, dvs med $2^n \equiv_3 1$, $3^n \equiv_7 1$ och $4^n \equiv_{41} 1$. Villkoret är precis att $n$ skall vara en multipel av 2:s (multiplikativa) ordning i $\mathbb{Z}_3$, 3:s ordning i $\mathbb{Z}_7$ och 4:s ordning i $\mathbb{Z}_{41}$.
Eftersom antalet element i den multiplikativa gruppen till $\mathbb{Z}_{41}$ är 40, är ordningen för 4 en delare till 40, dvs 1, 2, 4, 5, 8, 10, 20 eller 40. $4^1 = 4$, $4^2 = 16$, $4^4 = 16^2 = 10$, $4^5 = 4 \cdot 10 = 40 = -1$, $4^8 = 10^2 = 18$, $4^{10} = (-1)^2 = 1$ i $\mathbb{Z}_{41}$, så ordningen för 4 i $\mathbb{Z}_{41}$ är 10. P.s.s. (enklare) fås att ordningen för 3 i $\mathbb{Z}_7$ är 6 och för 2 i $\mathbb{Z}_3$ 2. Villkoret på $n$ blir alltså att $2, 6, 10 \mid n$, dvs att $30 \mid n$. **Svar: Alla positiva multipler av 30.**

**9a)** i) 0,1,2,3,3,4,5,6 : **möjligt**, se figuren till höger.
ii) 2,3,4,4,4,5,5,6 : **omöjligt**, ty summan av valenserna skall vara 2 gånger antalet kanter, dvs ett jämnt tal.
iii) 1,1,2,3,4,5,6,6 : **omöjligt**, ty 6-hörnen måste vara grannar med varsitt av 1-hörnen och båda med 2-hörnet. 5-hörnet får då bara fyra möjliga grannar.



**b)** Det gäller att visa att den bipartita grafen med $X$ = tentanderna och $Y$ = uppgifterna, kanter mellan en tentand och de uppgifter hon klarat, har en fullständig matchning.
Varje tentand har klarat minst fyra uppgifter, så det har varje icke-tom mängd tentander också totalt. Om det är fler än fyra tentander har de tillsammans klarat alla uppgifter (mindre än sex tentander kvar). Halls villkor är alltså uppfyllt, **saken är klar!**
**c)** Om vi adderar alla hörnens valenser räknar vi varje kant två gånger, så $3v = 2e$. Om vi adderar antalet kanter vid varje yta räknar vi p.s.s. varje kant två gånger, så $\sum_i ir_i = 2e$. Totala antalet ytor är $r = \sum_i r_i$.
För en plan, sammanhängande graf gäller Eulers polyederformel $v - e + r = 2$, så $3v - 3e + 3r = 6$. Med $3v = 2e$ ger det $-e + 3r = 6$, så $6r - 2e = 12$. Insättning av $r$ och $e$ ger $6 \sum_i r_i - \sum_i ir_i = \sum_i (6 - i) r_i = 12$. **Saken är klar.**

**10a)** Man finner med polynomdivision (i $\mathbb{Z}_3[x]$):
$2x^5 + 2x^4 + x^2 + 2 = (2x^2 + x + 2)(x^3 + 2x^2 + x + 2) + x^2 + 2x + 1$, så
**Svar: Kvoten är $2x^2 + x + 2$ och resten $x^2 + 2x + 1$.**
**b)** För att $\pi^3$ skall vara $id$ måste $(i_1\, i_2 \ldots i_k)^3 = id$ för varje cykel i $\pi$, dvs $\pi$ innehåller bara 1-cykler och 3-cykler (skriven med disjunkta cykler, förstås). Cykelstrukturen kan vara $[1^8]$, $[1^5\, 3]$, $[1^2\, 3^2]$. Antalen permutationer av varje typ fås med uttrycket längst ner sidan 134 i Biggs (eller direkta kombinatoriska resonemang). De är 1, 112 ,1120, så totalt 1+112+1120 = 1233 st. **Svar: 1233 st.**
**c)** Vi använder Burnsides lemma (Thm 21.4 i Biggs).
(Den regelbundna) tetraederns grupp av symmetrirotationer har 12 element: Identitetselementet (bevarar alla konfigurationer, $|F(id)| = k^6$), åtta rotationer $\pm\frac{2\pi}{3}$ kring axlar genom ett hörn och mittpunkten av motstående sidoyta (bevarar konfigurationer med samma färg på kanterna vid hörnet och samma på kanterna vid sidoytan, $|F(g)| = k^2$) och tre rotationer $\pi$ kring axlar genom mittpunkterna av motstående kanter (bevarar konfigurationer med övriga fyra kanter parvis likfärgade, $|F(g)| = k^4$).
Lemmat ger antalet väsentligt olika färgningar, **svar:** $\frac{1}{12}(k^6 + 3k^4 + 8k^2)$