KTH Matematik
B.Ek

Lösningar tentamen 5B1204 Diskret matematik för D2, 26 augusti 2005

Teoridelen

1a) Karakteristiska ekvationen måste ha dubbelroten $x = 2$. Enklaste (icke-triviala) ekvationen blir $(x-2)^2 = x^2 - 4x + 4 = 0$, dvs $x^2 = 4x - 4$, så
svar: Rekursionsekvationen $a_{n+2} = 4\,a_{n+1} - 4\,a_n$. (Se stencilen om rekursion.)
b) Se Biggs 15.4. **c)** $\sum_{v\in V}\delta(v) = 2\,|E|$, se Biggs 15.3.
2a) Se Biggs 17.6. **b)** Eulers polyederformel $v - e + r = 2$ ger med $v = 127, e = 266$ att $r = 141$, så **svaret: 141 ytor**. (Se stencilen om planära grafer.) **c)** Se Biggs 7.2.
3a) Se Biggs 5.2. **b)** På $\binom{n}{r} = \frac{n!}{r!\,(n-r)!}$ sätt, se Biggs 11.1.
c) Villkoret är precis att σ och π skall vara konjugerade. Det är de, eftersom de har samma cykelstruktur. Med $\pi = (14)(2)(365)$ fås $\tau\pi\tau^{-1} = (\tau(1)\tau(4))(\tau(2))(\tau(3)\tau(6)\tau(5))$, så detta blir $\sigma = (153)(26)(4)$ om man t.ex. tar $\tau = (124653)$, se Biggs 12.5.
4a) $\phi(539) = \phi(7^2\cdot 11) = 7^2\cdot 11(1-\frac{1}{7})(1-\frac{1}{11}) = 7\cdot 6\cdot 10 = 420$, se Biggs 11.5.
b) Om $\mathrm{sgd}(a,m) = 1$ gäller att $m \mid (ax - ay) = a(x-y) \Rightarrow m \mid x - y$, dvs $ax \equiv ay \pmod m \Rightarrow x \equiv y \pmod m$ och om $\mathrm{sgd}(a,m) = d \neq 1$ gäller att $m \mid a\frac{m}{d} - a\cdot 0$, men $m \nmid (\frac{m}{d} - 0)$, så det gäller då inte för alla x och y att $ax \equiv ay \pmod m \Rightarrow x \equiv y \pmod m$.
Svar: Villkoret är precis att a och m är relativt prima, $\mathrm{sgd}(a,m) = 1$.
c) Se stencilen om kinesiska restsatsen.
5a) Eftersom 41 är ett primtal är alla sådana grupper isomorfa med den cykliska gruppen C_{41}, så **svar: En**, se Biggs 20.8. **b)** Se Biggs 20.7.
c) En ring för alla $n \in \mathbb{N}$, se Biggs 22.1. En kropp precis då n är primtal, se Biggs 22.3 (om $n = a\cdot b$ med $a, b \neq \pm 1$ är $a\cdot b = 0, a, b \neq 0$ i $\mathbb{Z}_n$, så $\mathbb{Z}_n$ är inte en kropp).

Problemdelen

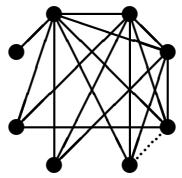
6a) Om H multipliceras med de mottagna orden (som kolonnvektorer) fås
$H\begin{bmatrix}1\\0\\0\\1\\1\end{bmatrix} = \begin{bmatrix}1\\1\\1\end{bmatrix}$, $H\begin{bmatrix}1\\0\\1\\1\\1\end{bmatrix} = \begin{bmatrix}0\\1\\0\end{bmatrix}$, $H\begin{bmatrix}1\\1\\1\\0\\0\end{bmatrix} = \begin{bmatrix}0\\0\\0\end{bmatrix}$, dvs H:s andra kolonn, H:s första kolonn och nollkolonnen. Fel har alltså inträffat i andra, första och ingen positionerna.
Svar: De sända orden var 11011, 00111 och 11100.
b) Det handlar tydligen om ett RSA–system med n' (vanligen kallat n) $= 1271 = 31\cdot 41, e = 107, m = (31-1)(41-1) = 1200$. Vi söker n (vanligen kallat d), så att $107\,n \equiv 1 \pmod{1200}$. Vi använder Euklides algoritm: $1200 = 11\cdot 107 + 23, 107 = 4\cdot 23 + 15, 23 = 1\cdot 15 + 8, 15 = 1\cdot 8 + 7, 8 = 1\cdot 7 + 1$, så $1 = 8 - 1\cdot 7 = 8 - (15 - 1\cdot 8) = -15 + 2\cdot 8 = -15 + 2(23 - 1\cdot 15) = 2\cdot 23 - 3\cdot 15 = 2\cdot 23 - 3(107 - 4\cdot 23) = -3\cdot 107 + 14\cdot 23 = -3\cdot 107 + 14(1200 - 11\cdot 107) = 14\cdot 1200 - 157\cdot 107 = (14-107)1200 + (1200-157)107 = 1043\cdot 107 - 93\cdot 1200$, så $1043\cdot 107 \equiv 1 \pmod{1200}$ och **svar: Vi kan ta** $n = 1043$. (I själva verket "räcker" $n = 203$.)
c) Låt $A_0 = \mathbb{N}$ och $n_0 = 0$. välj rekursivt för $i = 0, 1, 2, \ldots$ $A_{i+1} \subset A_i$ som en av $\{n \in A_i \mid n > n_i,\ \alpha_n$ har k i i:e positionen$\}$, $k = 0, 1$, så att A_{i+1} är oändlig (mängderna kan inte båda vara ändliga, eftersom deras union är A_i som (rekursivt) är oändlig) och låt n_{i+1} vara det minsta elementet i A_{i+1}. Då kommer alla $\alpha_{n_i}, \alpha_{n_{i+1}}, \ldots$ att vara lika i de i första positionerna, ty $n_i, n_{i+1}, \cdots \in A_i \subset A_{i-1} \subset \ldots$. **Saken är därmed klar.**
7a) Låt X vara mängden av möjliga placeringar. Det sökta antalet är då $|X|$ = antalet injektioner (olika barn på olika stolar) från en 13-mängd (barnen) till en 17-mängd (stolarna) $= (17)_{13} = 17\cdot 16\cdot \ldots \cdot 5 = \frac{17!}{4!}$. **Svar: Antalet placeringar är** $\frac{17!}{4!} (= 14820309504000)$**.**
b) Låt C vara mängden placeringar där Anna och Bo sitter bredvid varandra. Det sökta antalet är då $|X \setminus C| = |X| - |C|$. Men $|C| = 2\cdot (16)_{12} = 2\,\frac{16!}{4!}$ (2 ordningar mellan Anna och Bo, de båda ses som ett stort barn av 12, då finns totalt 16 positioner).
Svar: Antalet tillåtna placeringar är $\frac{17!}{4!} - 2\,\frac{16!}{4!} (= 10\cdot 15! = 13076743680000)$**.**
c) Låt A, B vara mängderna placeringar där Bo och Cecilia respektive Anna och Cecilia sitter bredvid varandra. Det sökta antalet är då (sållprincipen) $|X \setminus (A \cup B \cup C)| = |X| - (|A| + |B| + |C|) + (|A\cap B| + |B\cap C| + |C\cap A|) - |A\cap B\cap C|$. Som i **b)** är $|A| = |B| = |C| = 2\,\frac{16!}{4!}$, medan $|A\cap B| = |B\cap C| = |C\cap A| = 2\cdot (15)_{11} = 2\,\frac{15!}{4!}$ (om Cecilia sitter bredvid både Anna och Bo, sitter de tre i rad med Cecilia i mitten, 2 möjliga sätt, som ett extra stort barn av 11, totalt 15 positioner) och $|A\cap B\cap C| = 0$ (om Cecilia sitter bredvid Anna och Bo, sitter Anna inte bredvid Bo).
Svar: Antalet tillåtna placeringar är $\frac{17!}{4!} - 6\,\frac{16!}{4!} + 6\,\frac{15!}{4!} - 0 (= 182\,\frac{15!}{4!} = 9916530624000)$**.**

8a) Eftersom $\phi(15) = 15(1-\frac{1}{3})(1-\frac{1}{5}) = 8$ och $\text{sgd}(13,15) = 1$ är $13^8 \equiv_{15} 1$ (enligt Eulers sats). Således är $13^{1066} = 13^{8\cdot 133+2} \equiv_{15} 1^{133}13^2 \equiv_{15} (-2)^2 = 4$. Eftersom $0<4<15$ fås **svaret: Resten blir 4.**

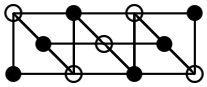
b) $25x \equiv_{63} 43 \Leftrightarrow 63 \mid (25x-43) \Leftrightarrow 63 \mid -5(25x-43) \Leftrightarrow 63 \mid ((2\cdot 63-125)x+(215-4\cdot 63)) \Leftrightarrow 63 \mid (x-37) \Leftrightarrow x \equiv_{63} 37$ (vi har använt att $\text{sgd}(-5,63) = 1$). (Man kan förstås använda Euklides algoritm för att finna $25^{-1} = 58 = -5$ i $\mathbb{Z}_{63}$.) **Svar: Alla** $x = 37 + 63\,t$, $t \in \mathbb{Z}$.

c) Låt $B = A+10 (= \{n+10 \mid n \in A\})$ och $C = A+20$. Det gäller att visa att $A \cap B \cap C \neq \varnothing$. Antag, för att få en motsägelse, att $A \cap B \cap C = \varnothing$. Då är $A \cup B \cup C \subseteq \{1, 2, \ldots, 1020\}$ och (sållprincipen) $|A \cup B \cup C| = |A| + |B| + |C| - (|A \cap B| + |B \cap C| + |C \cap A|)$. Men $A \cap B$ och $C \cap A$ är disjunkta delmängder till A, så $|A| \geq |A \cap B| + |C \cap A|$ (+1, men det behöver vi inte) och på samma sätt $|B| \geq |A \cap B| + |B \cap C|$ och $|C| \geq |C \cap A| + |B \cap C|$. Genom att addera får man $|A| + |B| + |C| \geq 2(|A \cap B| + |B \cap C| + |C \cap A|)$, dvs $-(|A \cap B| + |B \cap C| + |C \cap A|) \geq -\frac{1}{2}(|A| + |B| + |C|)$ och alltså $1020 \geq |A \cup B \cup C| \geq |A| + |B| + |C| - \frac{1}{2}(|A| + |B| + |C|) = \frac{1}{2} \cdot 3\,|A| = \frac{3}{2}681 > 1021$. Antagandet ledde till motsägelse, så **saken är klar.**
(En mer detaljerad analys visar att det räcker med färre än 681.)

9a) Låt hörnens valenser vara $1, 3, 3, 4, 5, 6, 7, x$. Summan av valenserna skall vara 2 gånger antalet kanter, ett jämnt tal, så x är udda och ≤ 7. $x = 1$ är omöjligt, ty hörnen med valenser 6,7 medför att det går minst 3 kanter till varje par av hörn. $x = 7$ är också omöjligt, ty två hörn med valens 7 skulle innebära att alla hörn hade valens minst 2. $x = 3, 5$ går båda, se fig. **Svar: Det åttonde hörnet kan ha valens 3 eller 5.**



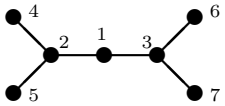
b) Enligt figuren är grafen bipartit. Eftersom den har ett udda antal hörn kan den inte ha någon hamiltoncykel (en sådan måste ha vartannat svart och vitt hörn, dvs lika många av vardera), **svar: Nej**.



c) Antag att grafen kan ritas plan. Då har varje yta minst 5 kanter, så summan av antalet kanter i ytorna är $\geq 5r$ (beteckningar enligt stencilen om planära grafer), men det är också $= 2e$ (varje kant räknas två gånger). Vi har alltså $2e \geq 5r$, så $r \leq \frac{2}{5}e$ och enligt Eulers formel för planära grafer $2 \leq 1 + c = v - e + r \leq v - \frac{3}{5}e$, så $e \leq \frac{5}{3}(v-2) = \frac{5}{3}(81-2) = 131\frac{2}{3}$. Men $e = 133$, motsägelse, så **svar: Nej grafen kan inte vara planär.**
($e \leq 131$ är bästa möjliga uppskattning, ty 5 dodekaedrar ihopklistrade yta mot yta ger en planär graf med 80 hörn och 130 kanter. Ett hörn till med en kant ger en planär graf med $v = 81, e = 131$)

10a) $f(x) = x^4 + 2x^2 + x + 2$ har enligt faktorsatsen en förstagradsfaktor precis om det har ett nollställe. $f(0) = 2$, men $f(1) = 0$, så $f(x)$ är delbart med $x - 1 = x + 2$. Division ger att $f(x) = (x+2)g(x)$ med $g(x) = x^3 + x^2 + 1$. Vi söker på samma sätt nollställen till $g(x)$. ($g(0) \neq 0$ eftersom $f(0) \neq 0$ och) $g(1) = 0$, så $g(x) = (x+2)h(x)$, där division ger $h(x) = x^2 + 2x + 2$. $h(1) = 2, h(2) = 1$, så $h(x)$ saknar förstagradsfaktor och är alltså (liksom $x+2$) irreducibelt. **Svar:** $f(x) = (x+2)^2(x^2+2x+2)$

b) (2p) Vi numrerar pärlorna som i figuren. Gruppen av "tillåtna" permutationer av pärlorna är då $G = \{(1), (45), (67), (45)(67), (23)(46)(57), (23)(47)(56), (23)(4657), (23)(4756)\}$, med $|G| = 8$.



Enligt Burnsides lemma (Thm 21.4 i boken) är antalet väsentligt olika färgningar = antalet banor för gruppens verkan på färgningarna $= \frac{1}{|G|}\sum_{g \in G} |F(g)|$. Om $g \in G$ som permutation har cykelstrukturen $[1^{\alpha_1}\, 2^{\alpha_2} \cdots]$, är $|F(g)|$, antalet färgningar som är invarianta under g:s verkan, $= \alpha_1 \cdot 2^{\alpha_1+\alpha_2+\ldots-1}$ (alla pärlor i samma cykel måste ha samma färg, den röda pärlan kan vara vilken som av 1-cyklerna och övriga cykler kan var och en färgas vit eller svart). Eftersom vi har 1 element av typ $[1^7]$, 2 av typ $[1^5\, 2^1]$, 1 av typ $[1^3\, 2^2]$, 2 av typ $[1^1\, 2^3]$ och 2 av typ $[1^1\, 2^1\, 4^1]$ blir det sökta antalet $\frac{1}{8}(1 \cdot 7 \cdot 2^6 + 2 \cdot 5 \cdot 2^5 + 1 \cdot 3 \cdot 2^4 + 2 \cdot 1 \cdot 2^3 + 2 \cdot 1 \cdot 2^2) = 7 \cdot 2^3 + 5 \cdot 2^3 + 3 \cdot 2 + 2 + 1 = 105$.
Svar: På 105 olika sätt.

c) För ett godtyckligt $a \in R$ gäller $a \cdot a = a$ och $(a+a) \cdot (a+a) = a + a$. Med axiom för en ring (distributivitet) fås $(a+a)\cdot(a+a) = (a+a)\cdot a + (a+a)\cdot a = (a\cdot a + a\cdot a) + (a\cdot a + a\cdot a) = (a+a) + (a+a) = a + a$. Eftersom $(R, +)$ är en grupp ger detta att $a + a = 0$, så (a var godtyckligt) **saken är klar**.