**Mathematics, KTH**
B.Ek

**Suggested solutions exam TEN1 SF2736 DISCRETE MATHEMATICS**
**January 13 2016**

There may be misprints.

**1)** (3p) We shall decide if there is an $n \in \mathbb{Z}_+$ with $233^n \equiv_{2310} 1$ and if so, find the least one.

**Solution:**
$2310 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$ and $233 \equiv_2 1$, $233 \equiv_3 2$, $233 \equiv_5 3$, $233 \equiv_7 2$, $233 \equiv_{11} 2$, so by the Chinese remainder theorem $233^n \equiv_{2310} 1 \Leftrightarrow (1^n \equiv_2 1,\ 2^n \equiv_3 1,\ 3^n \equiv_5 1,\ 2^n \equiv_7 1,\ 2^n \equiv_{11} 1)$. Checking for each module gives $233^n \equiv_{2310} 1 \Leftrightarrow 1, 2, 4, 3, 10 \mid n \Leftrightarrow \text{lcm}(1, 2, 4, 3, 10) = 60 \mid n$. The least such $n \in \mathbb{Z}_+$ is $n = 60$.

**Answer: Such $n$ do exist. The least one is $n = 60$.**

---

**2a)** $H = \begin{bmatrix} 1&1&1&0&0 \\ 0&0&1&0&1 \\ 1&0&1&1&0 \end{bmatrix}$ is the check matrix of a linear, binary code. We want the numbers of words (a, 2p) in the code and (b, 1p) which can not result from at most one error in a codeword.

**Solution:**
a. The rows of $H$ are linearly independant (as seen from columns 2, 4 and 5), so the dimension of the code is $k = n - \text{rank}\, H = 5 - 3 = 2$ and the number of codewords is $2^k = 4$.
b. Since all columns in $H$ are different and not the zero column, the code corrects one error. To every codeword there belong six words (the codeword and the five words resulting from one error in it) and no word belongs to two different codewords (since the code corrects one error). The total number of words which result from a codeword with at most one error is thus $4 \cdot 6$ and the ones we look for are the rest, $2^5 - 4 \cdot 6 = 8$ in number.
(Alt: Those containing more than one error are exactly the solutions of $H\mathbf{x} = \mathbf{c}$, where $\mathbf{c}$ is one of the two nonzero columns which are not in $H$. Four solutions for every $\mathbf{c}$.)

**Answer a: The code contains 4 words, b: There are 8 such words.**

---

**3)** (3p) 10 persons are to receive three cards each, one or two out of 15 white, indistinguishable ones and one or two out of 15 coloured, distinguishable ones.
We want the number of ways the 30 cards can be distributed.

**Solution:**
Since each person is to receive at least one white card, we start by giving them one.
The 5 persons with two white cards can then be chosen in $\binom{10}{5}$ ways.
Then the 15 coloured cards can be distributed with two to 5 of the persons and one to the others, in $\binom{15}{2,2,2,2,2,1,1,1,1,1}$ ways (distinct elements in distinct boxes).
The total number of ways is (by the multiplication principle) $\binom{10}{5} \cdot \binom{15}{2,2,2,2,2,1,1,1,1,1} = \frac{10!}{5! \cdot (10-5)!} \cdot \frac{15!}{2!^5}$.

**Answer: In $\frac{10! \cdot 15!}{5!^2 \cdot 2^5}$ $(= 10\,297\,935\,648\,000)$ ways.**

---

**4)** (3p) We have $x^2 a = bxc^{-1}$ and $acx = xac$ in a group $G$ and want $x$ expressed in $a, b, c$.

**Solution:**
$x^2 a = bxc^{-1} \overset{\cdot c}{\Rightarrow} x^2 ac = bx \overset{acx = xac}{\Rightarrow} xacx = bx \overset{\cdot x^{-1}}{\Rightarrow} xac = b \overset{\cdot (ac)^{-1}}{\Rightarrow} x = b(ac)^{-1}$.

**Answer: $x = b(ac)^{-1} (= bc^{-1}a^{-1})$.**

---

**5)** (3p) We shall show that if $k \in \mathbb{Z}_+$ edges of a Hamiltonian graph $G = (V, E)$ are deleted, the resulting graph will have at most $k$ components.

**Solution:**
The Hamiltonian cycle connects all the vertices. We delete at most $k$ of the edges in the cycle and thereby split the cycle into at most $k$ components (obvious, or induction: $k = 1$ gives a path (connected) and each removal of one edge splits at most one component into two).
Vertices in the same component of what was the cycle are in the same component of the resulting graph, so it has at most $k$ components. **We are done.**

---

**6)** $\pi, \sigma \in S_8$ are $\pi = (1\,7\,5\,6\,8)(2\,3\,4)$ and $\sigma = (1\,4\,7\,8\,6\,5\,3)$. $H$ is the set of products of $\pi$'s and $\sigma$'s and we shall show that (a, 2p) $H$ is a subgroup of $S_8$ and (b, 2p) $|H| \geq 420$.

**Solution:**
a. To show that $H$ is a subgroup, it is (by a well-known theorem, $H$ being finite ($H \subseteq S_8$ and $|S_8| = 8!$)) enough to show S0. $H \neq \varnothing$ and S1. $a, b \in H \Rightarrow ab \in H$.
S0: $id \in H$, S1: if $a$ and $b$ are both finite products of $\pi$'s and $\sigma$'s, so is $ab$. (More formally, it can be shown by induction (corresponding to the recursive definition of $H$) on the structure of the second factor.)
b. The order of a permutation is the lcm of the lengths of its cycles, so $o(\pi) = \operatorname{lcm}(5, 3) = 15$ and $o(\sigma) = 7$. That doesn't give the result we want, but $\pi\sigma = (1\,7\,5\,6\,8)(2\,3\,4)(1\,4\,7\,8\,6\,5\,3) = (1\,2\,3\,7)(4\,5) \in H$ has order $o(\pi\sigma) = \operatorname{lcm}(4, 2) = 4$.
The order of an element of a group always divides the order of the group, so $15, 7, 4 \mid |H|$, implying $\operatorname{lcm}(15, 7, 4) = 15 \cdot 7 \cdot 4 = 420 \mid |H|$, so $(|H| \geq 1 \Rightarrow) |H| \geq 420$. **We are done.**

---

**7)** (4p) We want a set $A \subseteq \mathbb{Z}_+$ such that for any $n \in \mathbb{Z}_+$ the numbers of partitions

$$p\Big(n \mid \text{for all } k \in \mathbb{Z}_+ : \begin{cases} \text{if } k \text{ is odd: at most one part of size } k, \\ \text{if } k \text{ is even: any number of parts of size } k \end{cases}\Big) =$$
$$= p(n \mid \text{the size of every part is in } A).$$

**Solution:**
The generating function of the numbers in the left-hand side is

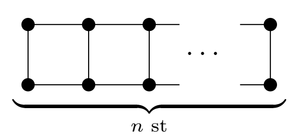
$$\prod_{k\,>\,0,\text{ odd}} (1 + x^k) \cdot \prod_{k=1}^{\infty} \frac{1}{1-x^{2k}} = \prod_{k\,>\,0,\text{ odd}} \frac{(1+x^k)}{(1+x^k)(1-x^k)} \cdot \prod_{k\,>\,0,\text{ even}} \frac{1}{(1-x^{2k})} =$$
$$= \prod_{k\,>\,0,\text{ odd}} \frac{1}{1-x^k} \cdot \prod_{k\,>\,0,\ 4\,\mid\,k} \frac{1}{1-x^k},$$

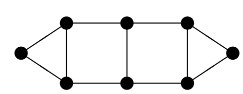
the generating function of the numbers in the right-hand side iff $A$ is the set of $k$ in the last products. (Remember, there is no problem with convergence of the infinite products. To contribute to a given $x^n$, only a finite number of factors are $\neq 1$.)

**Answer:** $\boldsymbol{A = \{k \in \mathbb{Z}_+ \mid k \not\equiv 2 \pmod 4\}}$**.**

---

**8)** $G_n$ is the upper graph and $P_n(\lambda)$ its chromatic polynomial. We want (a, 1p) $P_1(\lambda)$ and $P_2(\lambda)$, (b, 2p) $P_n(\lambda)$ for arbitrary $n = 1, 2, \ldots$ and (c, 1p) the number of ways to vertex colour the lower graph with at most 4 colours.



**Solution:**
$G_1$ consists of two vertices with an edge between them. The first vertex can be coloured in $\lambda$ ways and then the other in $\lambda - 1$ ways, so $P_1(\lambda) = \lambda(\lambda - 1)$.
The recursion formula for chromatic polynomials, $P_G(\lambda) = P_{G-e}(\lambda) - P_{G/e}(\lambda)$, with the rightmost edge as $e$, gives $P_{k+1}(\lambda) = P_k(\lambda)(\lambda - 1)^2 - P_k(\lambda)(\lambda - 2)$ (2 extra vertices with one neighbour each, give the factor $(\lambda - 1)^2$ and 1 vertex with 2 neighbours of different colours, gives $(\lambda - 2)$), so $P_{k+1}(\lambda) = P_k(\lambda)(\lambda^2 - 3\lambda + 3)$. With $P_1(\lambda)$ above, that gives $P_n(\lambda) = \lambda(\lambda - 1)(\lambda^2 - 3\lambda + 3)^{n-1}$.
The lower graph consists of a $G_3$ with 2 extra verices, each with 2 neighbours of different colours, so its chromatic polynomial is $P(\lambda) = P_3(\lambda)(\lambda - 2)^2$. The number of ways to vertex colour the graph with at most 4 colours is thus $P(4) = 4(4-1)(4^2 - 3 \cdot 4 + 3)^2(4-2)^2 = 4 \cdot 3 \cdot 7^2 \cdot 2^2 = 2\,352$.

**Answer a:** $\boldsymbol{P_1(\lambda) = \lambda(\lambda - 1),\ P_2(\lambda) = \lambda(\lambda - 1)(\lambda^2 - 3\lambda + 3)}$**,**
**b:** $\boldsymbol{P_n(\lambda) = \lambda(\lambda - 1)(\lambda^2 - 3\lambda + 3)^{n-1}}$**, c: The number of ways is 2 352.**

---

**9)** 20 children stand in a line. We want the number of possible orders among them if (a, 2p) Harry and Draco may not have exactly one child between them and (b, 3p) if, in addition, Ron and Draco may not have exactly one child between them.

**Solution:**

a. The desired number is (by the addition priciple) the number of ways to order them (20!) - the number of those ways **with** exactly one child between Harry and Draco ($2 \cdot 18 \cdot 18!$ (Harry or Draco first? (2), which child between them? (18), ways to order those three together and the remaining 17? (18!))).

b. With $X$ = the set of all orders of the 20 chidren, $A_1$ = the set of orders **with** exactly one child between Harry and Draco and $A_2$ = the set of orders **with** exactly one child between Ron and Draco, the principle of exclusion/inclusion gives the desired number: $|X \setminus (A_1 \cup A_2)| = |X| - |A_1| - |A_2| + |A_1 \cap A_2|$. As in a) $|X| = 20!$ and $|A_1| = |A_2| = 2 \cdot 18 \cdot 18!$. In a similar way: $|A_1 \cap A_2| = 2 \cdot 17 \cdot 16 \cdot 16!$ (Harry or Ron first? (Draco must be between them) (2), which of the other 17 children between Harry and Draco? (17), which of the remaining 16 children between Ron and Draco? (16), ways to order those five and the other 15? (16!)).

So, the desired number is $20! - 2 \cdot 18 \cdot 18! - 2 \cdot 18 \cdot 18! + 2 \cdot 17 \cdot 16 \cdot 16!$.

**Answer a: In $\mathbf{20! - 2 \cdot 18 \cdot 18! (= 2\,202\,416\,554\,770\,432\,000)}$ ways,**
**b: In $\mathbf{20! - 4 \cdot 18 \cdot 18! + 2 \cdot 17 \cdot 16 \cdot 16! (= 1\,983\,313\,099\,063\,296\,000)}$ ways.**

---

**10)** We want the number of non-isomorphic digraphs $G = (V, A)$ with (a, 3p) $|V| = 3$ and (b, 2p) $|V| = 4$. (A digraph is $G = (V, A)$, where $V$ is a set and $A \subseteq V \times V$.)

**Solution:**

a. A digraph with vertices $V$ with $|V| = 3$ is given exactly by a 0/1-matrix (each element 0 or 1) of type $3 \times 3$ and two such matrices give isomorphic digraphs iff one is obtained from the other by permuting rows and columns with the same permutation from $S_3$. Thus we want the number of orbits (corresponding to the isomorphism classes of digraphs) when $S_3$ acts by permuting rows and columns simultaneously in 0/1-matrices of type $3 \times 3$.

We use Burnside's lemma (Thm 21.4 in Biggs) and need $|F(\pi)|$ for all $\pi \in S_3$.

$|S_3| = (3! =)6$, elements of three types: $[1^3]$ (only $id$), $[12]$ (3 of them) and $[3]$ (2 of those).

Conjugate $\pi \in S_3$ (i.e. of the same type) have the same $|F(\pi)|$ and we find for one permutation of each type: $id$ fixes every matrix, so $|F(id)| = 2^9$,

$(1\,2)$ fixes a matrix iff elements with the same letter have the same value in $\begin{bmatrix} a & b & c \\ b & a & c \\ d & d & e \end{bmatrix}$, so $|F((1\,2))| = 2^5$ and $(1\,2\,3)$ fixes them according to $\begin{bmatrix} a & b & c \\ c & a & b \\ b & c & a \end{bmatrix}$, so $|F((1\,2\,3))| = 2^3$.

The number of orbits is $\frac{1}{|S_3|} \sum_{\pi \in S_3} |F(\pi)| = \frac{1}{6}(2^9 + 3 \cdot 2^5 + 2 \cdot 2^3) = \frac{8}{3}(32 + 6 + 1) = 104$.

b. Like in a), but with $S_4$ instead of $S_3$. In a table:

| Type: | $[1^4]$ | $[1^2 2]$ | $[13]$ | $[2^2]$ | $[4]$ |
|---|---|---|---|---|---|
| Number of such: | 1 | 6 | 8 | 3 | 6 |
| One such $\pi$: | $id$ | $(1\,2)$ | $(1\,2\,3)$ | $(1\,2)(3\,4)$ | $(1\,2\,3\,4)$ |
| $\pi$ fixes: | $\begin{bmatrix} a & b & c & d \\ e & f & g & h \\ i & j & k & l \\ m & n & o & p \end{bmatrix}$ | $\begin{bmatrix} a & b & c & d \\ b & a & c & d \\ e & e & f & g \\ h & h & i & j \end{bmatrix}$ | $\begin{bmatrix} a & b & c & d \\ c & a & b & d \\ b & c & a & d \\ e & e & e & f \end{bmatrix}$ | $\begin{bmatrix} a & b & c & d \\ b & a & d & c \\ e & f & g & h \\ f & e & h & g \end{bmatrix}$ | $\begin{bmatrix} a & b & c & d \\ d & a & b & c \\ c & d & a & b \\ b & c & d & a \end{bmatrix}$ |
| $\lvert F(\pi)\rvert$ | $2^{16}$ | $2^{10}$ | $2^6$ | $2^8$ | $2^4$ |

The number of orbits: $\frac{1}{|S_4|} \sum_{\pi \in S_4} |F(\pi)| = \frac{1}{24}(2^{16} + 6 \cdot 2^{10} + 8 \cdot 2^6 + 3 \cdot 2^8 + 6 \cdot 2^4)(= 3\,044)$.

**Answer a: 104, b: $\mathbf{\frac{1}{24}(2^{16} + 6 \cdot 2^{10} + 3 \cdot 2^8 + 8 \cdot 2^6 + 6 \cdot 2^4)(= 3\,044)}$.**

(These are also the numbers of non-isomorphic binary relations on a set $X$ with $|X| = 3, 4$.)

(The exponent of 2 in the term corresponding to a certain type can be found more easily. They are the number of orbits when $\pi$ acts on the positions of the matrix as $(i, j) \mapsto (\pi(i), \pi(j))$. The number of elements of such an orbit is the order of this action, $\mathrm{lcm}(\ell_i, \ell_j)$, where $\ell_{i,j}$ are the lengths of the $\pi$-cycles containing $i, j$. The number of orbits (= the desired exponent) is then $\sum_{i,j} \frac{1}{\mathrm{lcm}(\ell_i, \ell_j)} = \sum \frac{\ell \cdot \ell'}{\mathrm{lcm}(\ell, \ell')} = \sum \gcd(\ell, \ell')$, where the two last sums are taken over all ordered pairs of $\pi$-cycles and $\ell, \ell'$ are the lengths of the two cycles in the pair. E.g. with $\pi$ of type $[1^2 23]$ ($|X| = 7$) one gets 16 terms, one 3, one 2, and the rest 1's, so the exponent is 19.)

---