Mathematics, KTH
B.Ek

Suggested solutions exam TEN1 SF2736 DISCRETE MATHEMATICS
March 16, 2016
There may be misprints.

1) (3p) We want the $n \in \mathbb{Z}_+$, $n \geq 2$, such that $x^{-1} = x$ for all invertible $x \in \mathbb{Z}_n$.

Solution:
With $n = \prod_{i=1}^{r} p_i^{k_i}$ (p_i distinct primes and all $k_i \in \mathbb{Z}_+$), the Chinese remainder theorem shows that $(\mathbb{Z}_n, +, \cdot) \approx \ldots \times (\mathbb{Z}_{p_i^{k_i}}, +, \cdot) \times \ldots$
That means that $x^2 = 1$ in $\mathbb{Z}_n$ iff $x^2 = 1$ in $\mathbb{Z}_{p_i^{k_i}}$ for all $i = 1, \ldots, r$.
$x \in \mathbb{Z}_n$ is invertible iff $\gcd(x, n) = 1$ iff $p_i \nmid x$ iff $x \in \mathbb{Z}_{p_i^{k_i}}$ is invertible for all $i = 1, \ldots, r$.
So, n has the desired property iff each $p_i^{k_i}$ has it.
If p_i is odd, $2 \in \mathbb{Z}_{p_i^{k_i}}$ is invertible and $2^2 = 1$ only in the case $p_i = 3$, $k_i = 1$.
$3 \in \mathbb{Z}_{2^k}$ is invertible and $3^2 = 1$ iff $k = 1, 2, 3$. Inspection shows that the condition is fullfilled for all x in these cases ($1^2, 3^2, 5^2, 7^2 \equiv_{2,4,8} 1$).
All wanted n are thus the products of one of 1, 2, 4, 8 and one of 1 and 3, except $1 \cdot 1$.

Answer: All such values are n = 2, 3, 4, 6, 8, 12, 24.

---

2) (3p) We know that $1234^{503} \equiv_{6767} 4083$ and want a $k \in \mathbb{Z}_+$ with $4083^k \equiv_{6767} 1234$.

Solution:
We recognize an RSA-system with $n = 6767$ and $e = 503$ and want d, here called k.
$6767 = 67 \cdot 101$, both primes, so $m = 66 \cdot 100 = 6600$ and d works if it satisfies $e \cdot d \equiv_{6600} 1$.
The Euclidean algorithm:
$6600 = 503 \cdot 13 + 61$
$503 = 61 \cdot 8 + 15$
$61 = 15 \cdot 4 + 1$
so
$1 = 61 - 4(503 - 8 \cdot 61) =$
$= -4 \cdot 503 + 33(6600 - 13 \cdot 503) =$
$= 33 \cdot 6600 - 433 \cdot 503 =$
$= (33 - 503) \cdot 6600 + (6600 - 433) \cdot 503 =$
$= -470 \cdot 6600 + 6167 \cdot 503$
Thus, we can take $d = 6167 (= k)$.

Answer: One such k is 6167. **(Another is 2867 (it is enough that $e \cdot d \equiv_{\mathrm{lcm}(66,100)} 1$).)**

---

3) (3p) Disa wants to spend 14 of 21 days of vacation on discrete maths and 7 in the pool. We want to find the number of ways to do that, when the first and the last day are to be spent on discrete maths, she doesn't want two consecutive days in the pool, she has 14 different (one-day-)chapters discrete maths which can be studied in any order and the pool days are all the same.

Solution:
The math days may be ordered among them in 14! ways. For each such ordering, the pool days can be inserted in $\binom{13}{7} = \frac{13!}{7! \cdot 6!}$ ways (13 available slots between math days, at most one pool day in each slot). The multiplication principle gives the wanted number of ways: $14! \cdot \frac{13!}{7! \cdot 6!}$.

Answer: Disa can plan her vacation in $\frac{14! \cdot 13!}{7! \cdot 6!}$ (= 149 597 947 699 200) ways.

---

4) (3p) We want all possible values among 1, 2, ..., 10 för $|G|$, when the group G has a $g \in G$ with $g^6 = (g^{-1})^6$ and $g \neq 1$ (the identity element of G).

Solution:
$g^6 = (g^{-1})^6 \Leftrightarrow g^{12} = 1$, so $o(g) = 2, 3, 4, 6$ or 12 (since $o(g) \mid 12$ and $g \neq 1$). Since $o(g) \mid |G|$, $|G| = 1$, 5, 7 are not possible. The other values are possible, easily seen with G cyclic.

Answer: The values 1, 5, 7 are impossible, 2, 3, 4, 6, 8, 9, 10 are possible.

---

5) (3p) A plane, connected graph divides the plane into regions. 1 of them has 10 edges, 3 have 5 edges, 4 have 4 edges and 7 have 3 edges. We want the number of vertices.

Solution:
There are $r = 1 + 3 + 4 + 7 = 15$ regions and $e = \frac{1}{2}(10 + 3 \cdot 5 + 4 \cdot 4 + 7 \cdot 3) = 31$ edges (summing the numbers of edges means counting each edge twice). Euler's polyhedron formula (for a plane connected graph) gives $2 = v - e + r = v - 31 + 15$, so there are $v = 2 + 31 - 15 = 18$ vertices.

Answer: The graph has 18 vertices.

---

6) $\alpha(1)=5$, $\alpha(2)=3$, $\alpha(3)=2$, $\alpha(4)=4$, $\alpha(5)=1$, $\beta(1)=5$, $\beta(2)=1$, $\beta(3)=3$, $\beta(4)=2$, $\beta(5)=4$ and we shall (a, 1p) give α and $\alpha\beta$ in cycle notation, (b, 1p) decide if $\alpha^6\beta\alpha^{-11}\beta^6$ is even or odd and (c, 2p) find a $\pi \in S_5$ such that $\beta\pi, (\beta\pi)^2, \ldots, (\beta\pi)^6$ are all distinct.

Solution:
a. We find $\boldsymbol{\alpha = (1\,5)(2\,3)(4) = (1\,5)(2\,3)}$ (since $\alpha(1)=5$, $\alpha(5)=1$, $\alpha(2)=3$ etc.). $\alpha\beta$ means "first β, then α" and so $\boldsymbol{\alpha\beta = (1)(2\,5\,4\,3) = (2\,5\,4\,3)}$ (since $\beta(1)=5$, $\alpha(5)=1$, $\beta(2)=1$, $\alpha(1)=5$ etc.).
b. α is an even permutation, since it contains an even number (2) of cycles of even length, so α^{-1} is also even. $\beta = (1\,5\,4\,2)(3)$ is odd (only one cycle of even length). Since $\alpha^6\beta\alpha^{-11}\beta^6$ is a product containing in all an odd number of β, it is odd (α being even).
c. All $\beta\pi, (\beta\pi)^2, \ldots, (\beta\pi)^6$ are distinct iff the order $o(\beta\pi) \geq 6$ ($\sigma = \tau$ iff $\sigma\tau^{-1} = id$). One solution (of several) is obtained by choosing $\beta\pi = (1\,2)(3\,4\,5)$ (of order $\mathrm{lcm}(2,3) = 6$). That gives $\pi = \beta^{-1}(\beta\pi) = (1\,2\,4\,5)(1\,2)(3\,4\,5) = (1\,4)(3\,5)$.

Answer a: $\boldsymbol{\alpha = (1\,5)(2\,3)}$, $\boldsymbol{\alpha\beta = (2\,5\,4\,3)}$, b: $\boldsymbol{\alpha^6\beta\alpha^{-11}\beta^6}$ is odd,
c: For example $\boldsymbol{\pi = (1\,4)(3\,5)}$.

---

7) (4p) $\alpha_1, \alpha_2, \ldots$ are infinite sequences of 0's and 1's. We shall show that there are $n_i \in \mathbb{Z}_+$, $i = 1, 2, \ldots$ with $n_1 < n_2 < \ldots$, such that all $\alpha_{n_i}, \alpha_{n_{i+1}}, \ldots$ are the same in the first i positions.

Solution:
We first pick an infinite set of indices such that all corresponding α's start with the same symbol, 0 or 1 (always possible) and let n_1 be the least element in that set. Then we can proceed with that set of indices in the same way considering the symbol in the second position, giving n_2 etc. More formally:
Let $A_0 = \mathbb{N}$, $n_0 = 0$ and recursively choose $A_{i+1} \subset A_i$ for $i = 0, 1, 2, \ldots$ as one of the two sets $\{n \in A_i \mid n > n_i,\ \alpha_n \text{ has } k \text{ in the } i\text{th position}\}$, $k = 0, 1$, such that A_{i+1} is infinite (the sets can't both be finite, since their union is $A_i \setminus \{n_i\}$, which is (by recursion) infinite) and let n_{i+1} be the least element of A_{i+1}. Then all $\alpha_{n_i}, \alpha_{n_{i+1}}, \ldots$ will have the same sequence of digits in the first i positions (since $n_i, n_{i+1}, \cdots \in A_i \subset A_{i-1} \subset \ldots$). **We are done.**

---

8) (4p) $m = \prod_i p_i^{k_i} \neq 1$, p_i distinct primes and $k_i \in \mathbb{Z}_+$. We want the number of orbits when $G = U_m$ (the group of invertible elements of $\mathbb{Z}_m$) acts on $\mathbb{Z}_m$ by multiplication.

Solution: (Replacing the solution first given here. Using the CRT should make it more clear.)
Let $m_i = p_i^{k_i}$ and (x_i) denote $(x_1, x_2, \ldots)$ (where $x_i \in \mathbb{Z}_{m_i}$). Then (by the isomorphism of the Chinese remainder theorem) we can identify $(\mathbb{Z}_m, \cdot)$ with the set of all such (x_i), with $(x_i)\cdot(y_i) = (x_i \cdot y_i)$. $(g_i) \in G = U_m$ iff $(g_i)^{-1}$ exists (in $\mathbb{Z}_m$) iff g_i^{-1} exists (in $\mathbb{Z}_{m_i}$) (for all i) iff $g_i \in G_i = U_{m_i}$ (all i). (x_i) and (y_i) are in the same G-orbit iff $y_i = g_i x_i$ (all i) for some $(g_i) \in G$, i.e. iff x_i and y_i are in the same G_i-orbit (all i). So, the G-orbits are described bijectively by their corresponding G_i-orbits and the number of G-orbits is the product of the numbers of G_i-orbits.
We first restrict ourselves to the case $m = p^k$ and then multiply the results for all i involved. Let $x = a \cdot p^r$ and $y = b \cdot p^s$, $p \nmid a, b$ (so $a, b \in G$), and $r, s \in \{0, 1, \ldots, k\}$ ($r, s = k$ means $x, y = 0$). Then x and y are in the same G-orbit iff $r = s$ (if $r = s$, $y = (ba^{-1})x$ ($ba^{-1} \in G$) and $gx = (ga)p^r$ ($ga \in G$)), so the number of G-orbits is $k + 1$.
So, for the given $m = \prod_i p_i^{k_i}$, there are $\prod_i (k_i + 1)$ orbits (the number of positive divisors of m; for each $d \mid m$, all x with $\gcd(x, m) = d$ form an orbit).

Answer: The number of orbits is $\boldsymbol{\prod_i (k_i + 1)}$

(Using Burnside's lemma: The number of G-orbits is $\frac{1}{|G|}\sum_{g\in G} |F(g)|$, where $|G| = \phi(m)$ (with Euler's ϕ-function). $F(g) = \{x \in \mathbb{Z}_m \mid gx = x\} = \{x \in \mathbb{Z}_m \mid (g-1)x = 0\} = \{\text{multiples in } \mathbb{Z}_m \text{ of } \frac{m}{\gcd(g-1,m)}\}$, $|F(g)| = \gcd(g-1, m)$.
As above, we first take $m = p^k$. Then we find the numbers of $g \in G$ with given $\gcd(g-1, m)$:

r	0	$1, 2, \ldots, k-1$	k
how many $g \in G$ have $gcd(g-1, m) = p^r$?	$p^k - 2p^{k-1}$	$p^{k-r} - p^{k-r-1}$	1

which give $\sum_{g\in G} |F(g)| = p^{k-1}(p-2)\cdot p^0 + \sum_{r=1}^{k-1} p^{k-r-1}(p-1)\cdot p^r + 1\cdot p^k = p^{k-1}(p-2) + (k-1)p^{k-1}(p-1) + p^k =$
$= p^{k-1}(p - 2 + (k-1)(p-1) + p) = p^{k-1}(p-1)(k+1) = \phi(p^k)(k+1)$.
The number of orbits for $m = p^k$ is therefore $k + 1$ and the answer as above.)

---

9) (5p) We want the number of ways to place 10 white (identical), 10 black (identical) and 10 (distinct) coloured marbles in three (distinct) boxes, when no box may be empty.

Solution:

The (distinguishable) coloured marbles can be placed in the three boxes in 3^{10} ways.
For the (non-distinguishable) white and black marbles the corresponding numbers of ways are $\binom{12}{2} = 66$ for each colour (unordered choice with repetition allowed of 10 elements (the marbles) among the three boxes). The total number of distributions of the marbles (including cases where one or two boxes are empty) is thus $3^{10} \cdot 66^2$ (by the multiplication principle).
Let A_i be the set of distributions where box i is empty. By the inclusion-exclusion principle the number of distributions to be subtracted is: $|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - (|A_1 \cap A_2| + |A_1 \cap A_3| + |A_2 \cap A_3|) + |A_1 \cap A_2 \cap A_3| = 3 \cdot 2^{10} \cdot 11^2 - 3 \cdot 1 + 0$.

Answer: There are $3^{10} \cdot 66^2 - 3 \cdot 2^{10} \cdot 11^2 + 3$ $(= 256\,845\,735)$ ways.

---

10) We want (a, 1p) the order $|G|$ of the full symmetry group of a cube, (b, 1p) the number of odd permutations in S_8 given by G's action on the vertices of the cube and (c, 3p) the number of chiral (i.e. distinct from their mirror images) colourings of the edges of a regular tetrahedron, using at most k colours.

Solution:

a. For a vertex x of the cube, the orbit consists of all the vertices, so $|Gx| = 8$. The stabilizer consists of all permutations of the neighbours of x (three rotations (including id) and three reflections), so $|G_x| = |S_3| = 6$. That gives $|G| = |Gx| \cdot |G_x| = 48$.
b. G contains 24 rotations. Their types as elements of S_8 are $[1^8]$ (id), $[1^2 3^2]$ (axis through vertices), $[4^2]$, $[2^4]$ (axis through centers of surfaces, $\frac{\pi}{2}$ or π), $[2^4]$ (axis through midpoints of edges), all with an even number of cycles of even length, so they are all even permutations. Reflection in a plane parallel to two surfaces gives type $[2^4]$, also an even permutation. This reflection times the rotations give all non-rotations of G (they are distinct and exactly 24 in number), so they are also all even. No permutation given by an element of G is odd.
c. Call the group of symmetry rotations of the tetrahedron G_r and its full symmetry group G_f. Chiral colourings are then exactly those whose orbits under G_f are the union of two orbits under G_r. The number of chiral colourings is thus 2·(the difference in numbers of orbits for G_r and G_f).
We use Burnside's lemma (Thm 21.4 in Biggs) and need $|F(g)|$ for all $g \in G_r$, G_f.
$|G_r| = 12$ (for a vertex x, $|G_r x| = 4$ ($G_r x = \{$the vertices$\}$) and $|(G_r)_x| = 3$ ($(G_r)_x$ rotations, axis through x)).

type of rotation g	number	type for the permutation of the edges	$\lvert F(g)\rvert = k^{\text{number of cycles}}$
id	1	$[1^6]$	k^6
axis edge-edge	3	$[1^2 2^2]$	k^4
axis vertex-side	8	$[3^2]$	k^2

For G_f there are also the same number (12) of non-rotations (as in b.). $|G_f| = 24$, corresponding to all permutations of the four vertices. For the "extra" elements (those in $G_f \setminus G_r$) we find:

type for the permutation of the vertices	number	type for the permutation of the edges	$\lvert F(g)\rvert = k^{\text{number of cycles}}$
$[1^2 2]$	6	$1^2 2^2$	k^4
$[4]$	6	$[24]$	k^2

By the lemma, the number of orbits for G_r: $\frac{1}{12}(k^6 + 3k^4 + 8k^2)$ and
the number of orbits for G_f: $\frac{1}{24}(k^6 + 3k^4 + 8k^2 + 6k^4 + 6k^2) = \frac{1}{24}(k^6 + 9k^4 + 14k^2)$.
So, the number of chiral colourings: $2 \cdot (\frac{1}{12}(k^6 + 3k^4 + 8k^2) - \frac{1}{24}(k^6 + 9k^4 + 14k^2)) =$
$= 2 \cdot \frac{1}{24}(k^6 - 3k^4 + 2k^2) = \frac{1}{12}k^2(k^2 - 1)(k^2 - 2)$.

Answer a: $|G| = 48$, b: None of the permutations are odd,
c: The number of chiral colourings is $\frac{1}{12}k^2(k^2 - 1)(k^2 - 2)$.