Mathematics, KTH
B.Ek

Suggested solutions exam TEN1 SF2736 DISCRETE MATHEMATICS
April 12 2017

There may be misprints.

1) (3p) We want all $x \in \mathbb{Z}$ with $x^{31} + 158x \equiv 191 \pmod{385}$.

Solution:
$385 = 5 \cdot 7 \cdot 11$, 5, 7, 11 primes, so $a \equiv_{385} b \Leftrightarrow (a \equiv_5 b,\ a \equiv_7 b$ and $a \equiv_{11} b)$, if $a, b \in \mathbb{Z}$.
By Fermat's theorem $a^p \equiv_p a$ if p is prime, giving
1. $x^{31} + 158x \equiv_5 191 \Leftrightarrow x^3 + 3x \equiv_5 1 \Leftrightarrow x \equiv_5 3$ or 4 (test all $x \in \mathbb{Z}_5$),
2. $x^{31} + 158x \equiv_7 191 \Leftrightarrow x + 4x \equiv_7 2 \Leftrightarrow x \equiv_7 6$ ($5^{-1} \cdot 2 = 3 \cdot 2 = 6$ in $\mathbb{Z}_7$) and
3. $x^{31} + 158x \equiv_{11} 191 \Leftrightarrow x + 4x \equiv_{11} 4 \Leftrightarrow x \equiv_{11} 3$ ($5^{-1} \cdot 4 = 9 \cdot 4 = 3$ in $\mathbb{Z}_{11}$).

3. gives $x = 3 + 11s$, some $s \in \mathbb{Z}$, which by 2. satisfies
$3 + 11s \equiv_7 6 \Leftrightarrow 4s \equiv_7 3 \Leftrightarrow s \equiv_7 6$ ($4^{-1} = 2$ in $\mathbb{Z}_7$), so
$x = 3 + 11(6 + 7t) = 69 + 77t$, some $t \in \mathbb{Z}$, which by 1. satisfies one of the following two
$69 + 77t \equiv_5 3 \Leftrightarrow 2t \equiv_5 4 \Leftrightarrow t \equiv_5 2$, so $x = 69 + 77(2 + 5n) = 223 + 385n$, $n \in \mathbb{Z}$ (arbitrary)
$69 + 77t \equiv_5 4 \Leftrightarrow 2t \equiv_5 0 \Leftrightarrow t \equiv_5 0$, so $x = 69 + 77(0 + 5n) = 69 + 385n$, $n \in \mathbb{Z}$ (arbitrary).

Answer: $\boldsymbol{x = 69 + 385n}$ **or** $\boldsymbol{x = 223 + 385n}$**,** $\boldsymbol{n \in \mathbb{Z}}$ **arbitrary.**

---

2) (3p) For $n \in \mathbb{N}$, $\mathcal{A}_n = \{B \subseteq \{1, 2, \ldots, n\} \mid x, y \in B \Rightarrow y \neq x \pm 1\}$ and (with $\prod_{x \in \varnothing} x = 1$)
$f(n) = \sum_{B \in \mathcal{A}_n} \prod_{k \in B} k^2$. We want to find and prove an expression for $f(n)$.

Solution:
Some tests ($\mathcal{A}_0 = \{\varnothing\}, f(0) = 1$, $\mathcal{A}_1 = \{\varnothing, \{1\}\}, f(1) = 1 + 1^2 = 2$, $\mathcal{A}_2 = \{\varnothing, \{1\}, \{2\}\}$,
$f(2) = 1 + 1^2 + 2^2 = 6$ and $f(4) = 120$ given) seem to indicate that $f(n) = (n+1)!$.
We prove it by induction.
Base: $f(0) = 1 = (0+1)!$, $f(1) = 2 = (1+1)!$, the assertion is true for $n = 0, 1$.
Step: Assume the assertion true for $n = k, k+1$.
Each element of $\mathcal{A}_{k+2}$ is of exactly one of the types 1. no $k+2$, i.e. an element of $\mathcal{A}_{k+1}$, and 2. with $k+2$, i.e. $B \cup \{k+2\}$ for a (unique) $B \in \mathcal{A}_k$ ($k+1$ is not allowed if $k+2$ is included).
So $\mathcal{A}_{k+2} = \mathcal{A}_{k+1} \cup \{B \cup \{k+2\} \mid B \in \mathcal{A}_k\}$ (disjoint union), giving $f(k+2) =$
$= f(k+1) + (k+2)^2 \cdot f(k) \overset{\text{ind.ass.}}{=} (k+2)! + (k+2)^2(k+1)! = ((k+2) + (k+2)^2)(k+1)! =$
$= (k+3)! = (k+2+1)!$. Thus, the assertion is true for $k+2$ if it is true for k and for $k+1$.
By the principle of induction the assertion is true for all $n \in \mathbb{N}$.

Answer: $\boldsymbol{f(n) = (n+1)!}$ **for all** $\boldsymbol{n \in \mathbb{N}}$**, as proved above.**

---

3) (3p) We want the number of ways to distribute 9 different books and 17 identical donuts among 6 (different) children, so that each child has at least one book and one donut.

Solution:
The books can be given in $6! \cdot S(9,6) = 6! \cdot 2646$ ways
(surjections {books} $\to$ {children}, the Stirling number
$S(9,6) = 2646$ from "Stirlings triangle" on the right).
The donuts can be distributed in $\binom{11+6-1}{5} = \frac{16!}{5! \cdot 11!}$ ways
(one donut for each child, then unordered selection with repetition of 11 among 6 children, choose 5 walls of 16 positions).

1
1 1
1 3 1
1 7 6 1
15 25 10 1
90 65 15 1
350 140 21
1050 266
2646

The multiplication principle gives the total number of distributions,
$6! \cdot 2646 \cdot \frac{16!}{5! \cdot 11!} = \frac{6 \cdot 2646 \cdot 16!}{11!}$.

Answer: The distribution can be made in $\boldsymbol{\frac{6 \cdot 2646 \cdot 16!}{11!}}$ **(= 8 321 564 160) ways.**

---

4) $(G,\cdot)$ is a group and H, K are finite subgroups of G. We want all possible values (with $|H|$, $|K|$ given) of (a, 1p) $|H\cap K|$ and (b, 2p) $|aH\cap bK|$, when $a,b\in G$.

Solution:

a. $H\cap K$ is a subgroup of H and of K, so $|H\cap K| \,\big|\, \gcd(|H|,|K|)$. For groups A, B, D with $|A|=a$, $|B|=b$, $|D|=d$ the example $G=A\times D\times B$, $H=A\times D\times\{1_B\}$, $K=\{1_A\}\times D\times B$ (with $|H|=ad$, $|K|=bd$, $|H\cap K|=d$) shows that all divisors of $\gcd(|H|,|K|)$ are possible.

b. $aH\cap bK$ can be $\varnothing$ (e.g. if $H=K=\{1\}$, $a\neq b$) and if $c\in aH\cap bK$, $cH=aH$, $cK=bK$ (left cosets are identical or disjoint), so $aH\cap bK=c(H\cap K)$ and $|aH\cap bK|=|H\cap K|$.

Answer: Possible are a: all divisors of $\gcd(|H|,|K|)$, b: the same, and also 0.

---

5) (3p) We want to order $1,2,\ldots,9$ around a circle, so that the sum of two neighbouring elements is never a multiple of 3, 5 or 7.

Solution:

The problem is solved by a Hamiltonian cycle in a graph with vertices numbered 1–9 and edges between allowed neighbours (i.e. $\{i,j\}$ is an edge iff $3,5,7\nmid(i+j)$). 1, 2 and 4 have only two neighbours in the graph, so their edges must be in the cycle. That gives the sequence 6, 2, 9, 4, 7, 1, 3. The remaining 8, 5 can only be added in that order (6 and 8 are not adjacent).

Answer: One order (essentially the only one) is 1, 3, 8, 5, 6, 2, 9, 4, 7.

---

6) We want (a, 2p) the number of essentially different bracelets with 6 coloured (k colours available) beads on a loop and (b, 2p) the number with at least one red and one blue bead.

Solution:

a. We use Burnside's lemma. Placing the bracelet with the beads in the vertices of a regular hexagon, we see that the group G acting on the set of configurations corresponds to the identity id, the elements $r,r^2,\ldots,r^5$ (where r is rotation $\frac{2\pi}{6}=\frac{\pi}{3}$ around an axis through the center of the hexagon and perpendicular to its plane) and three rotations π each of type s_1, s_2 (s_1 being rotation around an axis in the plane of the hexagon, through centres of two opposing edges and s_2 around an axis through two opposing vertices). $|F(g)|$, the number of configurations held fixed by g, are found to be as in the table:

type of g	number of such g	g's permutation of the beads	$\lvert F(g)\rvert$
id	1	$[1^6]$	k^6
r,r^5	2	$[6]$	k
r^2,r^4	2	$[3^2]$	k^2
r^3	1	$[2^3]$	k^3
s_1	3	$[2^3]$	k^3
s_2	3	$[1^2 2^2]$	k^4

The number of essentially different bracelets = the number of orbits under G's action = $\frac{1}{|G|}\sum_{g\in G}|F(g)|=\frac{1}{12}(1\cdot k^6+2k+2k^2+k^3+3k^3+3k^4)=\frac{1}{12}(k^6+3k^4+4k^3+2k^2+2k)$.

b. Let X be all colourings in a) and B those with **no** blue bead, R those with no red bead. Then we now want $|X\smallsetminus(B\cup R)|=|X|-|B|-|R|+|B\cap R|=f(k)-2\cdot f(k-1)+f(k-2)$, where $f(k)$ is the answer in a). It turns out to be $\frac{1}{2}(5k^4-20k^3+41k^2-38k+14)$.

Answer a: The number of such bracelets is $f(k)=\frac{1}{12}(k^6+3k^4+4k^3+2k^2+2k)$,
b: Now the number is $\frac{1}{2}(5k^4-20k^3+41k^2-38k+14)$.

(It is also ok to answer in b) without simplifying, e.g. starting $\frac{1}{12}(k^6-2(k-1)^6+(k-2)^6+\ldots)$)

---

7) (4p) $\pi \in S_{10}$ is given by the table $\begin{array}{c|cccccccccc} i & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ \hline \pi(i) & 9 & 7 & 10 & 4 & 8 & 1 & 2 & 5 & 6 & 3 \end{array}$.
We want the number of functions $f\colon \mathbb{N}_{10} \to \mathbb{N}_{10}$ with $f(\pi(i)) = \pi(f(i))$ for all $i \in \mathbb{N}_{10}$.

Solution:
In cycle notation $\pi = (1\ 9\ 6)(2\ 7)(3\ 10)(4)(5\ 8)$ ($\pi(1) = 9$, $\pi(9) = 6$, $\pi(6) = 1, \ldots$).
A function with the desired property is completely determined by its values for one element in each one of π's cycles ($f(\pi(i)) = \pi(f(i))$ etc.) and f has the property iff $f(i)$ is in an m-cycle, with $m \mid k$, if i is from a k-cycle ($f(i) = f(\pi^k(i)) = \pi^k(f(i))$).
The number of such f is $4 \cdot 7 \cdot 7 \cdot 1 \cdot 7 = 1372$ (possible choices of $f(1)$, $f(2)$, $f(3)$, $f(4)$, $f(5)$).

Answer: There are 1372 such functions.

---

8) (4p) We want $A \subseteq \mathbb{Z}_+$, such that (using Biggs' notation):

$$p\big(n \mid \text{for all } k \in \mathbb{Z}_+ : \begin{cases} \text{if } 3 \mid k\text{: an arbitrary number of parts of size } k, \\ \text{else: at most two parts of size } k \end{cases}\big) =$$
$$= p(n \mid \text{the size of every part is in } A).$$

Solution:
The generating function of the numders in the LHS is

$$\prod_{k>0,\,3\nmid k}(1 + x^k + x^{2k}) \cdot \prod_{k=1}^{\infty} \frac{1}{1-x^{3k}} = \prod_{k>0,\,3\nmid k} \frac{(1-x^{3k})}{(1-x^k)} \cdot \prod_{k=1}^{\infty} \frac{1}{1-x^{3k}} =$$
$$= \prod_{k>0,\,3\nmid k} \frac{1}{(1-x^k)} \cdot \prod_{k>0,\,3\mid k} \frac{1}{1-x^{3k}} = \prod_{k>0,\,\gcd(k,9)\neq 3} \frac{1}{1-x^k},$$

the generating function of the numders in the RHS iff A is the set of k in the last product.
(No problems of convergence, remember. Only a finite number of factors $\neq 1$ contribute to any specific x^n.)

Svar: $\boldsymbol{A = \{k \in \mathbb{Z}_+ \mid \gcd(k, 9) \neq 3\}}$.

---

9) $(G, *)$ and $(A, \circ)$ with identities I and e are groups (A abelian). G acts on the set A with $g(a \circ b) = g(a) \circ g(b)$ (for $g \in G$, $a, b \in A$). We shall (a, 3p) show that $(K, \odot)$ is a group, where $K = G \times A$ and $\odot$ is given by $(g_1, a_1) \odot (g_2, a_2) = (g_1 * g_2, g_1(a_2) \circ a_1)$ and (b, 2p) decide if $H_1 = G \times \{e\}$, $H_2 = \{I\} \times A$ are subgroups and normal subgroups of $(K, \odot)$.

Solution:
a. That $(K, \odot)$ is a group follows if the axioms for a group (G1–G4) are satisfied.
G1 (closure): $g_1 * g_2 \in G$ and $g_1(a_2) \circ a_1 \in A$ for all $g_1, g_2 \in G$, $a_1, a_2 \in A$ (G, A closed under $*$, $\circ$ and $g_1(a_2) \in A$). G1 $\surd$.
G2 (associativity): $\big((g_1, a_1) \odot (g_2, a_2)\big) \odot (g_3, a_3) = (g_1 * g_2, g_1(a_2) \circ a_1) \odot (g_3, a_3) =$
$= ((g_1 * g_2) * g_3, (g_1 * g_2)(a_3) \circ (g_1(a_2) \circ a_1))$ should equal $(g_1, a_1) \odot \big((g_2, a_2) \odot (g_3, a_3)\big) =$
$= (g_1, a_1) \odot (g_2 * g_3, g_2(a_3) \circ a_2) = (g_1 * (g_2 * g_3), g_1(g_2(a_3) \circ a_2) \circ a_1)$.
$(g_1 * g_2) * g_3 = g_1 * (g_2 * g_3)$ ($*$ associative),
$(g_1 * g_2)(a_3) \circ (g_1(a_2) \circ a_1) = \big(g_1(g_2(a_3)) \circ g_1(a_2)\big) \circ a_1$ (G acts on A, $\circ$ associative) and
$g_1(g_2(a_3) \circ a_2) \circ a_1 = \big(g_1(g_2(a_3)) \circ g_1(a_2)\big) \circ a_1$ (given property of G's action) G2 $\surd$.
G3 (identity): $(I, e) \odot (g, a) = (I * g, I(a) \circ e) = (g, a \circ e) = (g, a)$ and $(g, a) \odot (I, e) =$
$= (g * I, g(e) \circ a) = (g, e \circ a) = (g, a)$ (I, e identities, $I(a) = a$ (all $a \in A$), $g(e) = e$ (all $g \in G$) (from $e \circ g(e) = g(e) = g(e \circ e) = g(e) \circ g(e)$)), so (I, e) is an identity. G3 $\surd$.
G4 (inverse): $(g, a) \odot (g^{-1}, g^{-1}(a^{-1})) = (g * g^{-1}, g(g^{-1}(a^{-1})) \circ a) = (I, (g * g^{-1})(a^{-1}) \circ a) =$
$= (I, I(a^{-1}) \circ a) = (I, a^{-1} \circ a) = (I, e)$ ($^{-1}$ inverse in G or in A, G acts on A, $I(b) = b$, all $b \in A$),
$(g^{-1}, g^{-1}(a^{-1})) \odot (g, a) = (g^{-1} * g, g^{-1}(a) \circ g^{-1}(a^{-1})) = (I, g^{-1}(a \circ a^{-1})) = (I, g^{-1}(e)) =$
$= (I, e)$, so $(g^{-1}, g^{-1}(a^{-1}))$ is an inverse of (g, a). G4 $\surd$. **Thus, $\boldsymbol{(K, \odot)}$ is a group.**
b. H_1 and H_2 are subgroups of K (the bijections $\phi_1((g, e)) = g$, $\phi_2((I, a)) = a$ are isomorphisms with G and A, since $(g_1, e) \odot (g_2, e) = (g_1 * g_2, g_1(e) \circ e) = (g_1 * g_2, e)$ and $(I, a_1) \odot (I, a_2) = (I * I, I(a_2) \circ a_1) = (I, a_1 \circ a_2)$.
$(I, a) \odot H_1 = \{(g, a) \mid g \in G\}$ and $H_1 \odot (I, a) = \{(g, g(a)) \mid g \in G\}$ are not equal if $g(a) \neq a$ for some $g \in G$, so H_1 is not necessarily a normal subgroup.
$(g, a) \odot H_2 = \{(g, g(a') \circ a) \mid a' \in A\}$ and $H_2 \odot (g, a) = \{(g, a \circ a') \mid a' \in A\}$. Both are $\{g\} \times A$ (g acts as a bijection on A), so H_2 is normal.

Answer b: $\boldsymbol{H_1}$ and $\boldsymbol{H_2}$ are subgroups. $\boldsymbol{H_2}$ is normal, but $\boldsymbol{H_1}$ is not, in general.
(K is called a semidirect product of the groups G and A. The condition that A be abelian is not necessary (not used above). A more natural definition is $(g_1, a_1) \odot (g_2, a_2) = (g_1 * g_2, a_1 \circ g_1(a_2))$.)

---

10) (5p) $G = (V, E)$ is an infinite graph, E countable. We shall show that $i) \Leftrightarrow ii)$, when
$i)$: For every finite $X \subset V$, the number of edges with exactly one vertex in X is infinite or even,
$ii)$: There exists a set of cycles and (two-way) infinite paths, with every $e \in E$ in exactly one of them.

Solution:
$i) \Rightarrow ii)$: Let $\{e_k\}_{k \in \mathbb{N}}$ be an enumeration of E, $e_0 = \{v, v'\}$. By $i)$, with $X = \{v\}$, there is a least $k > 0$ with $v \in e_k$ and similarly for v'. These edges are combined with e_0 and this is repeated at each end of the successively formed paths. In that way we obtain a cycle containing e_0 (if some end vertex gets an edge to the other) or a doubly infinite path containing e_0. If all edges in the so formed cycle/path are taken from G, a new graph $G' = (V, E')$ is obtained, also satisfying $i)$ (for every finite $X \subset V$ (but maybe not for some infinite ones) there is an even number of edges in the cycle/path that contain exactly one vertex from X (those at the ends of connected stretches of X-vertices), so an even number of edges is taken from the corresponding edge set in G). Starting from $e_k \in E'$ with minimal k, create a new cycle/path as above. Repeat.
The set of all thus created cycles/paths (finite or infinite) shows that $ii)$ is fulfilled.
$ii) \Rightarrow i)$: As we saw, every cycle or doubly infinite path has, for finite $X \subset V$ an even number of edges with exactly one vertex from X. If $ii)$ is fulfilled the set of all such edges in E is a union of sets, each with an even number of elements, giving $i)$. **That's it.**
