Mathematics, KTH
B.Ek

Suggested solutions exam TEN1 SF2736 DISCRETE MATHEMATICS
April 5 2018
There may be misprints.

1) (3p) We want all $x \in \mathbb{Z}$ that satisfy $x^{1682} + 22\,x \equiv 1652 \pmod{3599}$ [$3599 = 59 \cdot 61$].

Solution:
By the Chinese remainder theorem $\mathbb{Z}_{3599} \cong \mathbb{Z}_{59} \times \mathbb{Z}_{61}$, with isomorphism $x \mapsto ([x]_{59}, [x]_{61})$, so we start by solving the equation mod 59 and mod 61 separately.
$\mathbb{Z}_{\mathbf{59}}$: $1682 = 58 \cdot 29$, $1652 = 59 \cdot 28$, so in $\mathbb{Z}_{59}$ the equation is $(x^{58})^{29} + 22\,x = 0$ and since 59 is a prime, Fermat's little theorem gives $x^{58} = \begin{cases} 0, & \text{for } x = 0, \\ 1, & \text{otherwise.} \end{cases}$
Solutions are thus $x = 0$ and all solutions of $1 + 22\,x = 0$, i.e. $x = -22^{-1}$.
The Euclidean algorithm: $59 = 22 \cdot 2 + 15$, $22 = 15 \cdot 1 + 7$, $15 = 7 \cdot 2 + 1$,
thus $1 = 15 - 2 \cdot (22 - 15) = -2 \cdot 22 + 3 \cdot (59 - 2 \cdot 22) = 3 \cdot 59 - 8 \cdot 22$ and $22^{-1} = -8$.
So, **mod 59** all solutions are given by $\boldsymbol{x \equiv_{59} 0}$ and $\boldsymbol{x \equiv_{59} 8}$.
$\mathbb{Z}_{\mathbf{61}}$: $1682 = 60 \cdot 28 + 2$, $1652 = 61 \cdot 27 + 5$, so in $\mathbb{Z}_{61}$ the equation is $x^{60 \cdot 28 + 2} + 22\,x = 5$ and since 61 is a prime, Fermat's little theorem gives $x^{28 \cdot 60 + 2} = x^2$ for all $x \in \mathbb{Z}_{61}$.
Thus, the equation is here $x^2 + 22x = 5 \Leftrightarrow (x + 11)^2 = 121 + 5 = 2^2 \Leftrightarrow (x + 9)(x + 13) = 0$.
So, **mod 61** all solutions are $\boldsymbol{x \equiv_{61} -9}$ and $\boldsymbol{x \equiv_{61} -13}$ (61 is prime, so $61 \mid a \cdot b \Leftrightarrow 61 \mid a$ or $61 \mid b$).
We find the solutions in $\mathbb{Z}$ using $y_1 \equiv_{59} 1$, $\equiv_{61} 0$ and $y_2 \equiv_{59} 0$, $\equiv_{61} 1$,
$y_1 = 61s \equiv_{59} 1 \Leftrightarrow 2s \equiv_{59} 1$ and we choose $s = 30$, so $y_1 = 61 \cdot 30 = 1830$ and
$y_2 = 59t \equiv_{61} 1 \Leftrightarrow 2t \equiv_{61} -1$ and we choose $t = 30$, so $y_2 = 59 \cdot 30 = 1770$.
All solutions (Chinese remainder theorem): $x \equiv_{3599} 0 \cdot 1830 - 9 \cdot 1770 = -15\,930 \equiv_{3599} 2065$,
$x \equiv_{3599} 0 \cdot 1830 - 13 \cdot 1770 = \ldots \equiv_{3599} 2183$, $x \equiv_{3599} 8 \cdot 1830 - 9 \cdot 1770 = \ldots \equiv_{3599} 2309$,
$x \equiv_{3599} 8 \cdot 1830 - 13 \cdot 1770 = \ldots \equiv_{3599} 2427$.

Answer: All such $\boldsymbol{x = y + 3599 \cdot n}$, $\boldsymbol{n \in \mathbb{Z}}$, where $\boldsymbol{y = 2065, 2183, 2309}$ or 2427.

---

2) For $f\colon X \to Y$, we let $f\text{“}\colon \mathcal{P}(X) \to \mathcal{P}(Y)$ be given by $f\text{“}(A) = \{f(a) \mid a \in A\}$. We shall decide which of '$=$', '$\subseteq$', '$\supseteq$' necessarily hold between (a, 1p) $f\text{“}(A \cup B)$ and $f\text{“}(A) \cup f\text{“}(B)$, (b, 1p) $f\text{“}(A \cap B)$ and $f\text{“}(A) \cap f\text{“}(B)$, (c, 1p) $f\text{“}(A \setminus B)$ and $f\text{“}(A) \setminus f\text{“}(B)$.

Solution:
a. $y \in f\text{“}(A \cup B) \Leftrightarrow y = f(x)$ for some $x \in A \cup B \Leftrightarrow y = f(x)$ for some $x \in A$ and/or $y = f(x)$ for some $x \in B \Leftrightarrow y \in f\text{“}(A)$ and/or $y \in f\text{“}(B) \Leftrightarrow y \in f\text{“}(A) \cup f\text{“}(B)$,
so '$=$' (and thus also '$\subseteq$', '$\supseteq$') hold in a.
b. $y \in f\text{“}(A \cap B) \Leftrightarrow y = f(x)$ for some $x \in A \cap B \Rightarrow y \in f\text{“}(A) \cap f\text{“}(B)$,
but $X = Y = \{a, b\}$, $A = \{a\}$, $B = \{b\}$, $f(a) = f(b) = a$ give $f\text{“}(A \cap B) = f\text{“}(\varnothing) = \varnothing$ and $f\text{“}(A) \cap f\text{“}(B) = A \cap A = A \neq \varnothing$, so '$\subseteq$', but neither '$=$' nor '$\supseteq$', necessarily holds in b.
c. $y \in f\text{“}(A) \setminus f\text{“}(B) \Leftrightarrow y \in f\text{“}(A)$, $y \notin f\text{“}(B) \Leftrightarrow y = f(x)$ for some $x \in A$, but not for any $x \in B$ (so for an $x \in A \setminus B$) $\Rightarrow y \in f\text{“}(A \setminus B)$,
but X, Y, f as in b. give $f\text{“}(A \setminus B) = f\text{“}(A) = A$ and $f\text{“}(A) \setminus f\text{“}(B) = A \setminus A = \varnothing \neq A$,
so '$\supseteq$', but neither '$=$' nor '$\subseteq$', necessarily holds in c.

Answer a: $=$, $\subseteq$, $\supseteq$, b: $\subseteq$, c: $\supseteq$ must hold, the others not.

---

3) (3p) We want the number of ways to place four girls and five boys on three red and six white chairs, so that at least one girl sits on a red chair (children and chairs distinguishable).

Solution:
The number we want is the total number of ways to place the children minus the number of ways with all girls on white chairs (the addition principle), i.e. $9! - (6)_4 \cdot 5! = 9! - \frac{6!}{2!} \cdot 5!$ ways (the number of bijections 9-set $\to$ 9-set and (multiplication principle) the number of injections 4-set (the girls) $\to$ 6-set (the white chairs) $\cdot$ the number of bijections 5-set (the boys) $\to$ 5-set (the chairs without girls)).

Answer: In $\boldsymbol{9! - \frac{6! \cdot 5!}{2}}$ ($\boldsymbol{= 319\,680}$) ways.

---

4) $\pi, \sigma \in S_9$ are given by the table on the right. We want (a, 1p) π, σ and $\pi\sigma$ on cycle form and shall (b, 2p) show that if the group G contains π and σ, G's order must be divisible by 180.

i	1	2	3	4	5	6	7	8	9
$\pi(i)$	2	3	1	5	6	7	4	9	8
$\sigma(i)$	4	8	1	9	2	3	7	5	6

Solution:
a. $\pi(1) = 2$, $\pi(2) = 3$, $\pi(3) = 1$ etc. give $\pi = (1\,2\,3)(4\,5\,6\,7)(8\,9)$ and $\sigma = (1\,4\,9\,6\,3)(2\,8\,5)$. Composition (first σ then π) gives $(\pi\sigma)(1) = \pi(\sigma(1)) = \pi(4) = 5$ etc, so $\pi\sigma = (1\,5\,3\,2\,9\,7\,4\,8\,6)$.
b. G is a group containing π and σ and thus also $\pi\sigma$. The order of a group is a multiple of the order of each element (from Lagrange's theorem) and the order of a permutation is the least common multiple of the lengths of the cycles. The orders of $\pi, \sigma, \pi\sigma$ are then $\operatorname{lcm}(3,4,2) = 12$, $\operatorname{lcm}(5,3,1) = 15$, $\operatorname{lcm}(9) = 9$. $|G|$ is divisible by all three, therefore also by $\operatorname{lcm}(12, 15, 9) = 180$. **We are done.**

Answer a: $\pi = (1\,2\,3)(4\,5\,6\,7)(8\,9)$, $\sigma = (1\,4\,9\,6\,3)(2\,8\,5)$, $\pi\sigma = (1\,5\,3\,2\,9\,7\,4\,8\,6)$, b: Shown above.

---

5) An RSA system has public (n, e), where $n = 4331$ [$= 61 \cdot 71$]. We want (a, 1p) those of $205, \ldots, 209$ that are possible for e and (b, 2p) a corresponding d-value for one of those e's.

Solution:
a. The condition for e is that $\gcd(m, e) = 1$, where (for $n = p \cdot q$ with p, q distinct primes) $m = \phi(n) = (p-1)(q-1) = 60 \cdot 70 = 4200 = 2^3 \cdot 3 \cdot 5^2 \cdot 7$.
Since $2 \mid 206, 208$ and $3 \mid 207$ and $5 \mid 205$ and $2, 3, 5, 7 \nmid 209$ the only possibility is $e = 209$.
b. A corresponding d is determined by $e \cdot d \equiv_m 1$.
The Euclidean algorithm: $4200 = 209 \cdot 20 + 20$, $209 = 20 \cdot 10 + 9$, $20 = 9 \cdot 2 + 2$, $9 = 2 \cdot 4 + 1$, so $1 = 9 - 4 \cdot 2 = 9 - 4(20 - 2 \cdot 9) = -4 \cdot 20 + 9 \cdot 9 = -4 \cdot 20 + 9(209 - 10 \cdot 20) = 9 \cdot 209 - 94 \cdot 20 = 9 \cdot 209 - 94(4200 - 20 \cdot 209) = -94 \cdot 4200 + 1889 \cdot 209$ and we can take $d = 1889$.

Answer a: The only possible $e = 209$, b: A corresponding $d = 1889$.
(It is in fact enough that $e \cdot d \equiv_{\operatorname{lcm}(p-1, q-1)} 1$, so all $d = 209 + 420k$, $k \in \mathbb{Z}_+$ can be used.)

---

6) (4p) $G = (V, E)$, $G_i = (V_i, E_i)$, $V = V_1 \cup V_2$, $V_1 \cap V_2 = \varnothing$ and $E_i = \{\{x, y\} \in E \mid x, y \in V_i\}$. We shall show that for the chromatic polynomials $P_G(\lambda) \leq P_{G_1}(\lambda) \cdot P_{G_2}(\lambda)$ holds for $\lambda \in \mathbb{N}$.

Solution:
Let $G' = (V, E_1 \cup E_2)$ (i.e., G with all edges with vertices in both V_1 and V_2 removed, so G' "is" G_1 and G_2 without edges between them). Then colourings of the parts G_1 and G_2 are independent, so $P_{G'}(\lambda) = P_{G_1}(\lambda) \cdot P_{G_2}(\lambda)$ for $\lambda \in \mathbb{N}$ (for each colouring of G_1 there are $P_{G_2}(\lambda)$ colourings of G_2). But the colourings of G are a subset of those of G', so $P_G(\lambda) \leq P_{G'}(\lambda)$. **We are done**.

---

7) X is an infinite set and $G = \{f : X \rightleftarrows X\}$. We shall show that (a, 1p) $(G, \circ)$ is a group ($\circ$ composition), with (b, 2p) $H = \{f \in G \mid |\{x \in X \mid f(x) \neq x\}| < \infty\}$ a subgroup, and (c, 1p) decide if H is a normal subgroup.

Solution:
a. $(G, \circ)$ is a group, because (by the definition of a group)

- $f, g \in G \Rightarrow f \circ g \in G$ (closure, the composition of two bijections is a bijection),
- $f, g, h \in G \Rightarrow f \circ (g \circ h) = (f \circ g) \circ h$ (associativity, for all functions (if both sides are defined)),
- $f \in G \Rightarrow f \circ id = id \circ f = f$, where $id \in G$ is the identity function ($id(x) = x$, all $x \in X$) (identity) and
- $f \in G \Rightarrow f^{-1} \in G$ and $f \circ f^{-1} = f^{-1} \circ f = id$ (inverse, f^{-1} exists since f is a bijection). □

b. H is a subgroup of G, because (well-known theorem)

- $H \subseteq G$ (by the definition of H), $H \neq \varnothing$ ($id \in H$),
- $f, g \in H \Rightarrow f \circ g \in H$ (since $\{x \in X \mid (f \circ g)(x) \neq x\} \subseteq \{x \in X \mid f(x) \neq x\} \cup \{x \in X \mid g(x) \neq x\}$ and A, B finite, $C \subseteq A \cup B \Rightarrow C$ finite) and
- $f \in H \Rightarrow f^{-1} \in H$ (since $\{x \in X \mid f^{-1}(x) \neq x\} = \{x \in X \mid f(x) \neq x\}$). □

c. H is a normal subgroup since $f \in G$, $h \in H \Rightarrow f \circ h \circ f^{-1} \in H$ ($\{x \in X \mid f(h(f^{-1}(x))) \neq x\} = \{f(x) \mid x \in X,\ h(x) \neq x\}$) and $fHf^{-1} \subseteq H$, $f^{-1}Hf \subseteq H \Rightarrow fH = Hf$.

Answer a,b: Shown above, c: H is a normal subgroup.

8) (4p) $G=(V,E)$ is a graph, $\mu(x)$, for $x\in V$, the average of the degrees of x's neighbours ($=0$ if $\delta(x)=0$). We shall show that $\sum_{x\in V}\mu(x)\geq\sum_{x\in V}\delta(x)$.

Solution:
For all $x\in V$, $\mu(x)=\sum_{y\in V_x}\frac{1}{\delta(x)}\,\delta(y)$, where $V_x=\{y\in V\mid\{x,y\}\in E\}$, x's neighbours, so $\sum_{x\in V}\mu(x)=\sum_{x\in V,\,y\in V_x}\frac{\delta(y)}{\delta(x)}=\sum_{\{x,y\}\in E}(\frac{\delta(y)}{\delta(x)}+\frac{\delta(x)}{\delta(y)})\geq\sum_{\{x,y\}\in E}2=2|E|=\sum_{x\in V}\delta(x)$, where we used that $a^2+\frac{1}{a^2}\geq 2$ for all $a\in\mathbb{R}\setminus\{0\}$ (since $(a-\frac{1}{a})^2\geq 0$). **We are done.**

---

9) We shall (a, 1p) with $D\colon F[\![x]\!]\to F[\![x]\!]$ (F a field) given by $D(A(x))=\sum na_n\,x^{n-1}$ for $A(x)=\sum a_n\,x^n\in F[\![x]\!]$ show that $D(A(x)B(x))=D(A(x))B(x)+A(x)D(B(x))$, for all $A(x),B(x)\in F[\![x]\!]$, (b, 2p) find the coefficients of $p_n(x)$ when $E(x)=\sum\frac{1}{n!}\,x^n\in\mathbb{R}[\![x]\!]$ and $p_0(x)=1$, $p_{n+1}(x)E(x)=x\,D(p_n(x)E(x))$ for $n\in\mathbb{N}$, and (c, 2p) express the Bell number B_n (the number of equivalence relations on an n-set) as a convergent infinite series.

Solution:
a. If $A(x)=\sum a_n\,x^n$, $B(x)=\sum b_n\,x^n$ the coefficient of x^n in $A(x)B(x)$ is $\sum_{k=0}^n a_kb_{n-k}$. The coefficient of x^{n-1} in the LHS is $n\sum_{k=0}^n a_kb_{n-k}$ and in the RHS: $\sum_{k=0}^n k\,a_kb_{n-k}+$ $+\sum_{k=0}^n a_k(n-k)b_{n-k}=\sum_{k=0}^n(k+(n-k))a_kb_{n-k}=$ that of the LHS, so LHS=RHS. □
b. Let $p_n(x)=\sum p_{n,k}x^k$. Then $p_{0,0}=1$, $p_{0,k}=0$ for $k>0$ and a. gives $p_{n+1}(x)E(x)=$ $=x(\sum kp_{n,k}x^{k-1}+\sum p_{n,k}x^k)E(x)=(\sum_{k=1}^\infty(kp_{n,k}+p_{n,k-1})x^k)E(x)$ (since $D(E(x))=E(x)$). So for all $n\in\mathbb{N}$, $p_{n+1,0}=0$, $p_{n+1,k}=p_{n,k-1}+kp_{n,k}$ for $k>0$.
With $p_{0,k}$ as above we get $p_{n+1,k}=0$ for $k=0$ and $k>n+1$, $p_{n+1,1}=p_{n+1,n+1}=1$ and $p_{n+1,k}=p_{n,k-1}+kp_{n,k}$ for $1<k<n+1$, so $p_{n,k}=S(n,k)$, the Stirling number (of the second kind). $p_n(x)$ is for $n\in\mathbb{Z}_+$ therefore the polynomial $\sum_{k=1}^n S(n,k)x^k$ (the generating polynomial of the Stirling numbers).
c. The equivalence relations on a set correspond bijectively to the partitions of the set (into equivalence classes), so $B_n=\sum_{k=1}^n S(n,k)=p_n(1)$, the number of partitions of an n-set.
By b. $p_n(x)E(x)=(x\,D)^nE(x)=(x\,D)^{n-1}\sum_{k=1}^\infty\frac{k}{k!}x^k=\ldots=\sum_{k=1}^\infty\frac{k^n}{k!}x^k$.
$x=1$ gives $p_n(1)\cdot E(1)(=B_n\cdot e)=\sum_{k=1}^\infty\frac{k^n}{k!}$ (the RHS is convergent since the LHS is).

Answer a: Shown above, b: $p_n(x)$'s x^k-coefficient is $S(n,k)$ ($=0$ if $k=0$ or $>n$), c: $B_n=\frac{1}{e}\sum_{k=1}^\infty\frac{k^n}{k!}$ (Dobiński's formula).

(One can show that $\sum_{k=2n+1}^\infty\frac{k^n}{k!}<e$, so $B_n=\lceil\frac{1}{e}\sum_{k=1}^{2n}\frac{k^n}{k!}\rceil$ (Comtet's formula) ($\lceil a\rceil$ = the least integer $\geq a$). Writing $x=e^t$ one finds for $n\in\mathbb{Z}_+$ that $\sum_{k=1}^n S(n,k)e^{kt}\cdot e^{e^t}=\frac{d^n}{dt^n}e^{e^t}$.)

10) The graph $G = (X \cup Y, E)$ is bipartite and $r(A)$ is (for $A \subseteq X$) the greatest number of elements of A that can be simultaneously matched with elements of Y. We shall (a, 3p) show that $r(A \cup B) + r(A \cap B) \leq r(A) + r(B)$ holds for all $A, B \subseteq X$ and (b, 2p) give an exemple with $<$ in the inequality.

Solution:

a. Let M, N be matchings between $A \cup B$, $A \cap B$ respectively and Y with $|M| = r(A \cup B)$, $|N| = r(A \cap B)$. Then there is a matching M' between $A \cup B$ and Y with $|M'| = |M|$ and $N \subseteq M'$, because

if $x \in A \cap B$ and $\{x, y\} \in N \setminus M$,

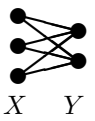
- add $\{x, y\}$ to M and exclude other edges of M that contain x or y,
- if $\{x, y'\}, \{x', y\} \in M$, also add $\{x', y'\}$ to M.

This gives a new matching of $A \cup B$ of the same size as M ($\not> |M|$ ($|M|$ is of maximal size), so at least one edge is excluded in the first step; iff two are excluded, one more is added in the second), containing $\{x, y\}$, and if this is repeated for all edges in $N \setminus M$ the desired M' is obtained (already added N-edges won't be affected again). □

Let matchings M_A, M_B between A, B and Y consist of the edges in M' containing vertices in A, B, respectively. Then $M_A \cup M_B = M'$ and $M_A \cap M_B = N$ ($|N| = r(A \cap B)$), so (sieve principle) $r(A \cup B) + r(A \cap B) = |M| + |N| = |M'| + |N| = |M_A| + |M_B| \leq r(A) + r(B)$. □

b. With $G = K_{3,2}$ as in the figure, and $A = \{1, 2\}$, $B = \{2, 3\}$ we find $r(A \cup B) = 2$, $r(A \cap B) = 1$, $r(A) = r(B) = 2$, so $r(A \cup B) + r(A \cap B) = 2 + 1 < 2 + 2 = r(A) + r(B)$. □

($G = K_{2,1}$ and $A = \{1\}$, $B = \{2\}$ works as well.)



Answer a: Shown above, b: Example above.

(A finite set $X \neq \varnothing$ with a function $r\colon \mathcal{P}(X) \to \mathbb{N}$, for alla $A, B \in \mathcal{P}(X)$ satisfying (like r above) the three conditions 1. $r(A) \leq |A|$, 2. $A \subseteq B \Rightarrow r(A) \leq r(B)$, and 3. the inequality in the problem, is called **a matroid**.

Other examples of matroids:

1. X a subset of a vector space, with $r(A) =$ the dimension of the subspace spanned by A,

2. $X = E$ for a graph $G = (V, E)$, with $r(A) =$ the maximal number of edges in A not containing a cycle.

An $A \in \mathcal{P}(X)$ satisfying $r(A) = |A|$ is called an **independent set**.)