Mathematics, KTH
B.Ek

Suggested solutions exam TEN1 SF2736 DISCRETE MATHEMATICS
January 12 2017

There may be misprints.

1) We want (a, 1p) the least (if there is one) $k \in \mathbb{Z}_+$ with $2^k \equiv_{1989} 1$ and (b, 2p) the largest $k \in \mathbb{Z}_+$ which is for some $x \in \mathbb{Z}$ the least with $x^k \equiv_{1989} 1$, and a corresponding x.

Solution:
By the Chinese remainder theorem $x^k \equiv_{1989} 1$ iff $x^k = 1$ in $\mathbb{Z}_9$, $\mathbb{Z}_{13}$, and $\mathbb{Z}_{17}$.
a. Powers of $[2]_9$, $[2]_{13}$, $[2]_{17}$:

k	1	2	3	4	5	6	7	8	9	10	11	12	13	
2^k	2	4	8	7	5	1	...							in $\mathbb{Z}_9$
2^k	2	4	8	3	6	12	11	9	5	10	7	1	...	in $\mathbb{Z}_{13}$
2^k	2	4	8	16	15	13	9	1	...					in $\mathbb{Z}_{17}$

This shows that $2^k \equiv_{1989} 1$ iff $k \mid 6, 12, 8$, i.e. iff $k \mid \operatorname{lcm}(6, 12, 8) = 24$.
The least such $k \in \mathbb{Z}_+$ is thus $k = 24$.
b. $x^k = 1$ in $\mathbb{Z}_{1989}$ iff $x \in U_{1989} \approx U_9 \times U_{13} \times U_{17}$ ($U_m = U(\mathbb{Z}_m)$, the invertible elements of $\mathbb{Z}_m$) and $o_m(x) \mid k$ for $m = 9, 13, 17$ (o_m: the multiplicative order in U_m). The least such k is therefore $\operatorname{lcm}(o_9(x), o_{13}(x), o_{17}(x))$.
We saw in a) that 2 has maximal order in $\mathbb{Z}_9$ and $\mathbb{Z}_{13}$ (namely $|U_9| = 6$ and $|U_{13}| = 12$), but $o_{17}(2) = 8 < |U_{17}| = 16$. Testing shows that $o_{17}(3) = 16$.
So, the wanted maximal $k = \operatorname{lcm}(6, 12, 16) = 48$ and $x \equiv_9 2, \equiv_{13} 2, \equiv_{17} 3$ gives a corresponding x. The first two give $x = 2 + 9 \cdot 13\,t$, $t \in \mathbb{Z}$. Also the last is satisfied if(f) $9 \cdot 13\,t \equiv_{17} 1$, i.e. $t \equiv_{17} 2 \cdot 4 = 8$ ($9^{-1} = 2$, $13^{-1} = 4$ in $\mathbb{Z}_{17}$) and $t = 8 + 17u$, $x = 2 + 9 \cdot 13 \cdot 8 + 9 \cdot 13 \cdot 17\,u = 938 + 1989\,u$, $u \in \mathbb{Z}$ arbitrary.

Answer a: $k = 24$, b: $k = 48$, one possible x is 938 (others are 5, 7, and 10).

(Shorter: $o_{17}(3^n) = 16$ if $\gcd(n, 16) = 1$. If $x \equiv_{17} 3^n$ and $x \in U_9$, U_{13} and further $3 \mid o_9(x)$ or $3 \mid o_{13}(x)$ then x is "corresponding". $n = 5$ gives $3^n \equiv_{17} 5$ and $o_9(5) = 6$, $o_{13}(5) = 4$ etc.)

---

2) (3p) A binary linear code $\mathcal{C}$ has $|\mathcal{C}| = 8$ and 101010, 111001, 110111 $\in \mathcal{C}$.
We want a check matrix H for $\mathcal{C}$ and to decide if $\mathcal{C}$ corrects one error.

Solution:
Length 6 and $|\mathcal{C}| = 8 = 2^3$ give $\operatorname{rank} H = 6 - 3 = 3$, so all H with 3 linearly independent rows satisfying Hc_i^T for $c_{1,2,3}$ the given words of $\mathcal{C}$ is a check matrix for $\mathcal{C}$. The rows of H are therefore any linearly independent solutions of the homogeneous system with coefficients $\left[\begin{smallmatrix}1&0&1&0&1&0\\1&1&1&0&0&1\\1&1&0&1&1&1\end{smallmatrix}\right] \overset{1 \text{ to } 2,3}{\sim} \left[\begin{smallmatrix}1&0&1&0&1&0\\0&1&0&0&1&1\\0&1&1&1&0&1\end{smallmatrix}\right] \overset{2 \text{ to } 3}{\sim} \left[\begin{smallmatrix}1&0&1&0&1&0\\0&1&0&0&1&1\\0&0&1&1&1&0\end{smallmatrix}\right] \overset{3 \text{ to } 1}{\sim} \left[\begin{smallmatrix}1&0&0&1&0&0\\0&1&0&0&1&1\\0&0&1&1&1&0\end{smallmatrix}\right]$.
By taking the last bits to be 100, 010, 001 we find the rows 101100, 011010, 010001, so $H = \left[\begin{smallmatrix}1&0&1&1&0&0\\0&1&1&0&1&0\\0&1&0&0&0&1\end{smallmatrix}\right]$. It has identical columns, so $\mathcal{C}$ does not correct one error, eg. $000000, 100100 \in \mathcal{C}$ both give 100000 with one error.

Answer: $H = \left[\begin{smallmatrix}\mathbf{1}&\mathbf{0}&\mathbf{1}&\mathbf{1}&\mathbf{0}&\mathbf{0}\\\mathbf{0}&\mathbf{1}&\mathbf{1}&\mathbf{0}&\mathbf{1}&\mathbf{0}\\\mathbf{0}&\mathbf{1}&\mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{1}\end{smallmatrix}\right]$ is a check matrix for $\mathcal{C}$, $\mathcal{C}$ doesn't correct one error.

---

3) (3p) We want the number of ways to spend 31 days on maths, novels, and gaming.
There are to be 9 days of gaming, never two in a row, and more days maths than novels.

Solution:
The number of days without gaming is $31 - 9 = 22$. They can be distributed between on maths and novels in 2^{22} ways, $\binom{22}{11}$ of them having the same number of days of each. Half of the rest, $\frac{1}{2}(2^{22} - \binom{22}{11})$, are the distributions with more days maths than novels.
The 23 slots between and before/after them can be filled by 9 days gaming in $\binom{23}{9}$ ways.
The multiplication principle gives the wanted number of distributions,
$\binom{23}{9} \cdot \frac{1}{2}(2^{22} - \binom{22}{11}) = \frac{23!}{9!\cdot 14!} \cdot (2^{21} - \frac{22!}{2\cdot(11!)^2})$.

Answer: Didrik can spend the days in $\frac{\mathbf{23!}}{\mathbf{9!\cdot 14!}} \cdot (\mathbf{2^{21} - \frac{22!}{2\cdot(11!)^2}})$ (= 1 425 535 654 840) ways.

4) $(G,\cdot)$ is a group and we are given the equations $a=b^2,\ b=c^2,\ c=a^2$ for $a,b,c\in G$. We want (a, 1p) all solutions with at least two of a,b,c equal and (b, 2p) to show that if $|G|=1467$ there are no solutions with all a,b,c distinct.

Solution:

a. Let a,b,c satisfy the equations and $b=a$ ($c=b$ and $a=c$ similar). Then $a=b^2=a^2$, so $a=1$, the identity of G (multiply by a^{-1}). Then also $b=a=1$ and $c=a^2=1$.

b. The equations give $a=b^2=(c^2)^2=c^4=(a^2)^4=a^8$, so $a^7=1$. Therefore $o(a)\mid 7$ and $o(a)=1$ or 7. $o(a)=1$ means $a=1$ and then $b=c=1$ (i.e. they are not distinct), while $o(a)=7$ is impossible since $o(a)\mid|G|$ and $7\nmid 1467$. **We are done.**

Answer a: The only such solution is $a=b=c=1$, b: Shown above.

---

5) (3p) A plane, connected graph has 2 vertices of degree 3, the rest of degree 4. 4 regions are bounded by 4 edges, the rest by 3. We want the numbers of vertices, edges and regions.

Solution:

Let (as usual) v, e, r be the numbers of vertices, edges and regions of the graph.

Euler's formula gives $v-e+r=2$. The sum of the degrees is $2e$, so $3\cdot 2+4(v-2)=2e$.

The same for the dual graph ($v^\perp=r$, $r^\perp=v$) gives $4\cdot 4+3(r-4)=2e$, leading to the system

$$\begin{cases} v-e+r=2\\ 2v-e=1\\ 2e-3r=4\end{cases}\quad\text{with the solution}\quad\begin{cases} v=9\\ e=17\\ r=10.\end{cases}$$

Answer: The graph has 9 vertices, 17 edges, and 10 regions.

---

6) $(G,*)$ is a group and $A\subseteq G,\ A\neq\varnothing$. We want to (a, 2p) show that $|G_A|\le|A|$ when $G_A=\{g\in G\mid a\in A\Rightarrow g*a\in A\}$, (b, 1p) show that G_A is a subgroup of G if A is finite, and (c, 1p) find G and A where G_A is not a group.

Solution:

a. follows from the fact that $g\in G_A$ is determined by its action on a single $a\in A$:

Take an $a_0\in A$ (exists since $A\neq\varnothing$). If $g_1,g_2\in G$ and $g_1*a_0=g_2*a_0$, then $g_1=g_2$ (since $a_0\in G$, multiply by a_0^{-1} from the right). That means that $f_0\colon G_A\to A$ given by $f_0(g)=g*a_0$ is an injection, so $|G_A|\le|A|$ (the pigeonhole principle; the definition of $\le$ if G_A is infinite).

b. $a\in A\Rightarrow 1*a\in A$, so $1\in G_A$ and $G_A\neq\varnothing$.

$g_1,g_2\in G_A\Rightarrow(a\in A\Rightarrow g_2*a\in A\Rightarrow g_1*(g_2*a)=(g_1*g_2)*a\in A)\Rightarrow g_1*g_2\in G_A$.

A finite gives G_A finite, so (known theorem) G_A is a subgroup of G.

c. With $(G,*)=(\mathbb{Z},+)$ and $A=\mathbb{N}$, $G_A=\mathbb{N}$, which is not a group under addition.

Answer a,b: Shown above, c: $(G,*)=(\mathbb{Z},+)$ and $A=\mathbb{N}$ form such an example.

---

7) (4p) For $m,n\in\mathbb{Z}_+$ we want to show that $\phi(d)\phi(mn)=d\phi(m)\phi(n)$, where $d=\gcd(m,n)$ and ϕ is Euler's function.

Solution:

Let, for $k\in\mathbb{Z}_+$, $P_k=\{p:p\text{ prime},\ p\mid k\}$. Then $\phi(k)=k\cdot\prod_{p\in P_k}(1-\frac{1}{p})$ (known fact).

Thus (for $m,n\in\mathbb{Z}_+$) $\phi(d)\phi(mn)=dmn\cdot\prod_{p\in P_d}(1-\frac{1}{p})\prod_{p\in P_{mn}}(1-\frac{1}{p})$ and

$d\phi(m)\phi(n)=dmn\cdot\prod_{p\in P_m}(1-\frac{1}{p})\prod_{p\in P_n}(1-\frac{1}{p})$.

Since $P_{mn}=P_m\cup P_n$, $P_d=P_m\cap P_n$ both expressions are dmn times factors $(1-\frac{1}{p})^2$ for p in both P_m and P_n and factors $(1-\frac{1}{p})$ for p in exactly one of P_m and P_n. Therefore they are equal. **We are done.**

---

8) (4p) $\sigma \in S_{13}$ is given by:

i	1	2	3	4	5	6	7	8	9	10	11	12	13
$\sigma(i)$	11	8	1	9	4	12	5	13	7	6	3	10	2

We want the number of $\pi \in S_{13}$ with $\pi\sigma = \sigma^{-1}\pi$.

Solution:
In cycle notation $\sigma = (1\ 11\ 3)(2\ 8\ 13)(4\ 9\ 7\ 5)(6\ 12\ 10)$ (since $\sigma(1) = 11$, $\sigma(11) = 3$, $\sigma(3) = 1, \ldots$).
$\pi\sigma = \sigma^{-1}\pi \Leftrightarrow \pi\sigma\pi^{-1} = \sigma^{-1}$. $\sigma^{-1} = (3\ 11\ 1)(13\ 8\ 2)(5\ 7\ 9\ 4)(10\ 12\ 6)$ and
$\pi\sigma\pi^{-1} = (\pi(1)\ \pi(11)\ \pi(3))(\pi(2)\ \pi(8)\ \pi(13))(\pi(4)\ \pi(9)\ \pi(7)\ \pi(5))(\pi(6)\ \pi(12)\ \pi(10))$.
They are equal iff the 3-cycles in one correspond to the 3-cycles in the other and the 4-cycles correspond to each other.
$\pi(1)$ can be any element of the 9 ones in the 3-cycles of σ^{-1}, it determines $\pi(11)$, $\pi(3)$,
$\pi(2)$ can then be chosen among 6 elements (2 3-cycles remain), it determines $\pi(8)$, $\pi(13)$,
$\pi(6)$ can then be chosen among 3 elements, it determines $\pi(12)$, $\pi(10)$ and at last
$\pi(4)$ can be chosen as any element in the 4-cycle of σ^{-1}, it determines $\pi(9)$, $\pi(7)$, $\pi(5)$.
In all, this gives (the multiplication principle) $9 \cdot 6 \cdot 3 \cdot 4 = 648$ possible π.

Answer: There are 648 different such π.

---

9) (5p) If $G = (V_G, E_G)$ is a graph, $\mathcal{R}$ an equivalence relation on V_G with equivalence classes $\mathcal{V}_i$, $i \in I$, the quotient graph $G/\mathcal{R} = (V_{G/\mathcal{R}}, E_{G/\mathcal{R}})$ is given by $V_{G/\mathcal{R}} = \{\mathcal{V}_i \mid i \in I\}$ and $E_{G/\mathcal{R}} = \{\{\mathcal{V}_i, \mathcal{V}_j\} \mid$ there are $v_i \in \mathcal{V}_i$, $v_j \in \mathcal{V}_j$ with $\{v_i, v_j\} \in E_G\}$.
We want to show that if $H = (V_H, E_H)$ is a connected graph, there is a tree $T = (V_T, E_T)$ and an equivalence relation $\mathcal{R}$ on V_T, such that $H \approx T/\mathcal{R}$ and $|E_H| = |E_T|$.

Solution:
Induction on $|V_H|$.
Base: If $|V_H| = 0$ or 1 we can take $T = (V_H, \varnothing)$, $\mathcal{R}$ the equality relation.
Step: Assume that the statement is true for all connected graphs with less vertices than H.
Let $|V_H| \geq 2$. Then there is an $x \in V_H$ such that $H' = (V_{H'}, E_{H'})$, formed by removing x and its edges from H, is connected (x can be a leaf of a spanning tree of H). By the assumption there is a tree $T' = (V_{T'}, E_{T'})$ with $|E_{H'}| = |E_{T'}|$, an equivalence relation $\mathcal{R}'$ on $V_{T'}$ and an isomorphism $\phi' \colon V_{H'} \to V_{T'/\mathcal{R}'}$.
Let x have neighbours $y_1, y_2, \ldots, y_k$, $k = \delta(x)$ in H. We form $T = (V_T, E_T)$ from T' by adding a vertex x_i and an edge $\{y_i, x_i\}$ for each y_i. T is then a tree (connected and without cycles) and $|E_H| = |E_{H'}| + k = |E_{T'}| + k = |E_T|$. Let $\mathcal{R}$ be $\mathcal{R}'$ with an extra new equivalence class $\mathcal{V}_x = \{x_i \mid i = 1, 2, \ldots, k\}$. $\mathcal{R}$ is an equivalence relation on V_T and $\phi = \phi' \cup \{(x, \mathcal{V}_x)\}$ is an isomorphism $H \to T/\mathcal{R}$ (if $u, v \in V_{H'}$: $\{u, v\} \in E_H \Leftrightarrow \{u, v\} \in E_{H'} \Leftrightarrow \{\phi'(u), \phi'(v)\} \in E_{T'/\mathcal{R}'} \Leftrightarrow$
$\Leftrightarrow \{\phi(u), \phi(v)\} \in E_{T/\mathcal{R}}$ and $\{u, x\} \in E_H \Leftrightarrow u = y_i$, for some $i \in \{1, \ldots, k\} \Leftrightarrow \{\phi(u), \mathcal{V}_x\} \in E_{T/\mathcal{R}} \Leftrightarrow$
$\Leftrightarrow \{\phi(u), \phi(x)\} \in E_{T/\mathcal{R}}$). **By the principle of induction we are done.**

---

10) (5p) We want the number of essentially different ways to colour the sides of a cube with as many red as blue sides, when there are also k other colours that may be used.

Solution:
To use Burnside's lemma we need $|F(g)|$ for each (type of) symmetry rotation g.

type of g	g's permutation of the cube's sides	number of g	$\lvert F(g)\rvert$
id	$[1^6]$	1	$k^6 + 30k^4 + 90k^2 + 20$
rot $vv \pm \frac{2\pi}{3}$	$[3^2]$	8	$k^2 + 2$
rot $ee\,\pi$	$[2^3]$	6	$k^3 + 6k$
rot $ss \pm \frac{\pi}{2}$	$[1^2\,4]$	6	$k^3 + 2k$
rot $ss\,\pi$	$[1^2\,2^2]$	3	$k^4 + 4k^2 + 4k + 4$

("rot $xx\,a$": rotation by an angle a with axis through cube's and sides'(s), edges'(k) or vertices'(h) centers.)
$|F(g)|$: the number of g-invariant (i.e. the same colour on all sides in the same cycle) colourings.
$|F(id)|$: no red/blue, one each $(\binom{6}{1,1,4} = 30)$, two each $(\binom{6}{2,2,2} = 90)$ or three each $(\binom{6}{3,3,0} = 20)$, in the other rows the cycles can be red/blue/other in a similar way,
$4k$ in the last row: the 1-cycles can be red and a 2-cycle blue or the other way around.
By the lemma, the number of ways: $\frac{1}{|G|}\sum_{g \in G} |F(g)| = \frac{1}{24}((k^6 + 30k^4 + 90k^2 + 20) + 8 \cdot (k^2 + 2) +$
$+ 6 \cdot (k^3 + 6k) + 6 \cdot (k^3 + 2k) + 3 \cdot (k^4 + 4k^2 + 4k + 4)) = \frac{1}{24}(k^6 + 33\,k^4 + 12\,k^3 + 110\,k^2 + 60\,k + 48)$.

Answer: The desired number is $\frac{1}{24}(k^6 + 33\,k^4 + 12\,k^3 + 110\,k^2 + 60\,k + 48)$.