Mathematics, KTH
B.Ek

Suggested solutions exam TEN1 SF2736 DISCRETE MATHEMATICS
January 11 2018

There may be misprints.

1) For how many $x \in \mathbb{Z}_{4851}$ is $x^{292} = 196$? [$4851 = 3^2 \cdot 7^2 \cdot 11$]

Solution:
By the Chinese remainder theorem, $\mathbb{Z}_{4851} \cong \mathbb{Z}_9 \times \mathbb{Z}_{49} \times \mathbb{Z}_{11}$, isomorphism $x \mapsto ([x]_9, [x]_{49}, [x]_{11})$.
$196 \equiv_9 7, \equiv_{49} 0, \equiv_{11} 9$, so $x^{292} \equiv_{4851} 196$ iff $x^{292} \equiv_9 7, \equiv_{49} 0, \equiv_{11} 9$.
For $a \in \mathbb{Z}_9$, $a^k = 0$ if $3 \mid a$ and $k \geq 2$, $a^6 = 1$ otherwise (sgd$(a, 9) = 1$; Euler's theorem, $\phi(9) = 6$).
Since $292 \equiv_6 4$ $a^{292} = a^4$ for all $a \in \mathbb{Z}_9$. That gives:

a	0	1	2	3	4	5	6	7	8
a^{292}	0	1	7	0	4	4	0	7	1

,

so $a^{292} = 7$ for **2** $\boldsymbol{a} \in \mathbb{Z}_{\mathbf{9}}$.
For $\boldsymbol{a} \in \mathbb{Z}_{\mathbf{49}}$, $a^k = 0$ iff $7 \mid a$, $k \geq 2$ (other a's are invertible), so $a^{292} = 0$ for **7** $\boldsymbol{a} \in \mathbb{Z}_{\mathbf{49}}$.
For $\boldsymbol{a} \in \mathbb{Z}_{\mathbf{11}}$, $a^k = 0$ if $a = 0$ and $k \geq 1$, $a^{10} = 1$ otherwise (Fermat's little theorem, 11 prime).
Since $292 \equiv_{10} 2$, $a^{292} = a^2$ if $a \in \mathbb{Z}_{11}$. That gives for $a \in \mathbb{Z}_{11}$:

a	0	1	2	3	4	5	6	7	8	9	10
a^{292}	0	1	4	9	5	3	3	5	9	4	1

,

so $a^{292} = 9$ for **2** $\boldsymbol{a} \in \mathbb{Z}_{\mathbf{11}}$.
As mentioned above, the elements of $\mathbb{Z}_{4851}$ are given by elements of $\mathbb{Z}_9 \times \mathbb{Z}_{49} \times \mathbb{Z}_{11}$, so there are $2 \cdot 7 \cdot 2 = 28$ $x \in \mathbb{Z}_{4851}$ which satisfy $x^{292} = 196$.

Answer: The desired number is 28.

---

2) (3p) $f\colon X \rightleftarrows X$ is a bijection on a finite set X. We shall decide if the relation $\mathcal{R}$ on X, for $x, y \in X$ given by $x\mathcal{R}y \Leftrightarrow y = f^n(x)$ for some $n \in \mathbb{Z}_+$, is an equivalence relation.

Solution:
f is a permutation of X (a bijection of X onto X), so each $x \in X$ is in a cycle (since $|X| < \infty$).
$\boldsymbol{\mathcal{R}}$ **is reflexive**, i.e. $x\mathcal{R}x$ for all $x \in X$, since if x is in a k-cycle $f^k(x) = x$,
$\boldsymbol{\mathcal{R}}$ **is symmetric**, i.e. $x\mathcal{R}y \Rightarrow y\mathcal{R}x$ for all $x, y \in X$, since if x is in a k-cycle and $y = f^i(x)$, $i \in \mathbb{Z}_+$, $x = f^j(y)$ for all j with $k \mid (i + j)$ (and such j exist in $\mathbb{Z}_+$),
$\boldsymbol{\mathcal{R}}$ **is transitive**, i.e. $(x\mathcal{R}y$ and $y\mathcal{R}z) \Rightarrow x\mathcal{R}z$ for all $x, y, z \in X$, since if $y = f^n(x)$ and $z = f^m(y)$ with $m, n \in \mathbb{Z}_+$, $z = f^{m+n}(x)$ and $m + n \in \mathbb{Z}_+$.
$\mathcal{R}$ is therefore reflexive, symmetric and transitive, thus (by definition) an equivalence relation.

Answer: Yes, $\boldsymbol{\mathcal{R}}$ is an equivalence relation on $\boldsymbol{X}$.

---

3) $A = \{1, 2, \ldots, 7\}$, $B = \{1, 2, \ldots, 13\}$ and we want (a, 2p) the number of $f\colon A \to B$ which take exactly 4 different values and (b, 1p) the number of them (i.e. the ones in a) which take at least one odd value.

Solution:
a. The taken values can be chosen in $\binom{13}{4} = \frac{13!}{4!\cdot(13-4)!}$ (the number of 4-subsets of a 13-set) ways and for each such choice there are $4! \cdot S(7, 4) = 4! \cdot 350$ (the Stirling number $S(7, 4) = 350$ by the diagram) surjections of A onto the set of the four values. The multiplikation principle gives the desired number, $\frac{13!\cdot 350}{9!}$.

1
1 1
1 3 1
1 7 6 1
15 25 10
90 65
350

b. By the addition principle, the desired number is obtained by subtracting the number of such functions that only take even values $(\binom{6}{4} \cdot 4! \cdot S(7, 4) = \frac{6!\cdot 350}{(6-4)!})$ from the answer in a. That gives $(\frac{13!}{9!} - \frac{6!}{2!}) \cdot 350$.

Answer a: $\boldsymbol{\frac{13!\cdot 350}{9!}}$ (= 6 006 000), b: $\boldsymbol{\left(\frac{13!}{9!} - \frac{6!}{2!}\right) \cdot 350}$ (= 5 880 000).

---

4) (3p) $(G,\cdot)$ is a group and $\varphi\colon G \to G$ is given by $\varphi(g) = g^{-1}$, all $g \in G$.
We shall show that φ is an isomorphism iff G is abelian.

Solution:
φ is an isomorphism iff it is a bijection and $\varphi(g_1g_2) = \varphi(g_1)\varphi(g_2)$ for all $g_1, g_2 \in G$.
We first show "if", so suppose the group G is abelian (i.e. commutative).
φ is a bijection, since it has the inverse $\varphi^{-1} = \varphi$ (since $(g^{-1})^{-1} = g$ for all $g \in G$).
If $g_1, g_2 \in G$, $\varphi(g_1g_2) = (g_1g_2)^{-1} = g_2^{-1}g_1^{-1} = \varphi(g_2)\varphi(g_1) \overset{G \text{ abelian}}{=} \varphi(g_1)\varphi(g_2)$. □
To show "only if", suppose φ is an isomorphism and let g_1, g_2 be arbitrary in G.
Since φ is a bijection, there are $h_1, h_2 \in G$ with $g_i = \varphi(h_i)$ ($i = 1, 2$) and $g_1g_2 = \varphi(h_1)\varphi(h_2) \overset{\varphi \text{ iso}}{=}$
$= \varphi(h_1h_2) = (h_1h_2)^{-1} = h_2^{-1}h_1^{-1} = \varphi(h_2)\varphi(h_1) = g_2g_1$. □ **We are done.**

5) $\pi, \sigma \in S_{13}$ are given by:
We want (a, 1p) the parities of π and σ and (b, 2p) all $n \in \mathbb{Z}$ satisfying $\tau\pi^n = \sigma^n\tau$ for some $\tau \in S_{13}$.

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

Solution:
a. On cycle form, $\pi = (1\ 9)(2\ 8\ 4\ 7\ 11\ 5)(3\ 12)(6)(10\ 13)$ ($\pi(1) = 9$, $\pi(9) = 1, \ldots$) and $\sigma = (1\ 11\ 6)(2)(3\ 12\ 7\ 4)(5)(8)(9\ 13\ 10)$. The types of $\pi :\ [1\ 2^3\ 6]$, $\sigma :\ [1^3\ 3^2\ 4]$.
The parities are π: even (4 (even) cycles of even length), σ: odd (1 (odd) cycle of even length).
b. $\tau\pi^n = \sigma^n\tau \Leftrightarrow \sigma^n = \tau\pi^n\tau^{-1}$, so we want $n \in \mathbb{Z}$ making π^n and σ^n conjugate, i.e. of the same type (by a well-known theorem).
The n-th power of a k-cycle is d $\frac{k}{d}$-cycles, $d = \text{sgd}(k, n)$, but we only need the cases $k = 1, 2, 3, 4, 6$ to construct this table of the types:

n	0	1	2	3	4	5	6	7	8	9	10	11	12
π^n	$[1^{13}]$	$[12^36]$	$[1^73^2]$	$[12^6]$	$[1^73^2]$	$[12^36]$	$[1^{13}]$	$[12^36]$	$[1^73^2]$	$[12^6]$	$[1^73^2]$	$[12^36]$	$[1^{13}]$
σ^n	$[1^{13}]$	$[1^33^24]$	$[1^32^23^2]$	$[1^94]$	$[1^73^2]$	$[1^33^24]$	$[1^92^2]$	$[1^33^24]$	$[1^73^2]$	$[1^94]$	$[1^32^23^2]$	$[1^33^24]$	$[1^{13}]$

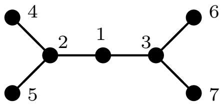
The table has period 12 in both directions (π, π^{-1} of the same type and $o(\pi) = 6$, $o(\sigma) = 12$) and we see that π^n and σ^n are of the same type iff $4 \mid n$.

Answer a: π is even and σ is odd, b: All $n = 4k$, $k \in \mathbb{Z}$.

6) (4p) $G = (V, E)$ is a plane, connected graph with $\delta(x) \geq 3$ for all $x \in V$ and the dual graph $G^\perp = (V^\perp, E^\perp)$ has $|V^\perp| \leq 11$. We shall show that $\delta^\perp(x) \leq 4$ for some $x \in V^\perp$.

Solution:
Suppose (for a contradiction) that $\delta^\perp(x) \geq 5$ for all $x \in V^\perp$.
The sum of the degrees in a graph is (common notation) $2\,|E|$, so $3v \leq \sum_{x\in V} \delta(x) = 2e$ and $5v^\perp \leq \sum_{x\in V^\perp} \delta^\perp(x) = 2e^\perp = 2e$ ($e = e^\perp$ by the definition of $G^\perp$).
Euler's polyhedron formula (plane, connected graph) and the number of regions $r = v^\perp$ (definition of $G^\perp$): $2 = v - e + r = v - e + v^\perp \leq v^\perp - \frac{e}{3}$, so $\frac{2e}{5} \geq v^\perp \geq 2 + \frac{e}{3}$. That gives $\frac{2e}{5} \geq 2 + \frac{e}{3}$, i.e. $(\frac{2}{5} - \frac{1}{3})e = \frac{e}{15} \geq 2$, so $e \geq 30$, and $v^\perp \geq 2 + \frac{e}{3} \geq 12$, contradiction. **We are done.**

7) (4p) We want the number of essentially different ways (i.e. so that they remain different however all or part of the arrangement is rotated) ways to colour the beads with exactly two red beads and the rest in k other colours.



Solution:

Numbering the beads as in the figure, the group of "allowed" permutations of them is $G = \{(1), (45), (67), (45)(67), (23)(46)(57), (23)(47)(56), (23)(4657), (23)(4756)\}$, $|G| = 8$. By Burnside's lemma (Thm 21.4 in the book) the number of essentially different colourings = the number of orbits of the action of the group on the colourings $= \frac{1}{|G|}\sum_{g\in G}|F(g)|$.

g	type	number of g's	$\lvert F(g)\rvert$
id	$[1^7]$	1	$\binom{7}{2}\cdot k^5 = 21\,k^5$
$(4\,5), (6\,7)$	$[1^5\,2]$	2	$1\cdot k^5 + \binom{5}{2}\cdot k^4 = k^5 + 10\,k^4$
$(4\,5)(6\,7)$	$[1^3\,2^2]$	1	$\binom{2}{1}\cdot k^4 + \binom{3}{2}\cdot k^3 = 2\,k^4 + 3\,k^3$
$(2\,3)(4\,6)(5\,7), (2\,3)(4\,7)(5\,6)$	$[1\,2^3]$	2	$\binom{3}{1}\cdot k^3 = 3\,k^3$
$(2\,3)(4\,6\,5\,7), (2\,3)(4\,7\,5\,6)$	$[1\,2\,4]$	2	k^2

$|F(g)|$ is found using that all beads in the same cycle must have the same colour and the two red beads can form two 1-cycles or one 2-cycle.

We find $\frac{1}{|G|}\sum_{g\in G}|F(g)| = \frac{1}{8}\big(21k^5 + 2(k^5+10k^4) + (2k^4+3k^3) + 2\cdot 3k^3 + 2k^2\big) =$
$= \frac{1}{8}(23\,k^5 + 22\,k^4 + 9\,k^3 + 2\,k^2)$

Answer: The desired number is $\frac{1}{8}(23\,k^5 + 22\,k^4 + 9\,k^3 + 2\,k^2)$.

($k = 1$ gives 7, $k = 2$ gives 146, $k = 3$ gives 954, $k = 4$ gives 3724 etc.)

8) (4p) $G = (V, E)$ is a connected graph.
We shall show that its edges can be directed so that at most one vertex has odd out-degree.

Solution:

A direction of the edges which minimizes $|\{x \in V \mid \delta^+(x) \text{ udda}\}|$ (one exists, since the number $\in \mathbb{N}$) satisfies the condition. Namely, if $x, y \in V$, $x \neq y$, $\delta^+(x), \delta^+(y)$ odd, change the direction of all edges in a path between x and y. Then $\delta^+(x), \delta^+(y)$ become even and the parity of all other out-degrees are unchanged, so the number of $x \in V$ with $\delta^+(x)$ odd decreases, contradiction. **We are done.**

9) (5p) We want the value of $\sum_{n=0}^{\infty} 2^{-n}\cdot F_n$, where the Fibonacci numbers $\{F_n\}_{n=0}^{\infty}$ are defined by $F_0 = 0$, $F_1 = 1$ and $F_{n+2} = F_{n+1} + F_n$ for $n \in \mathbb{N} = \{0, 1, 2, \ldots\}$.

Solution:

We use the series obtained from substituting $x = \frac{1}{2}$ in the generating function $\sum_{n=0}^{\infty} F_n\, x^n$ (a formal power series) to find its value and show that it converges.

Let $\phi = \frac{1+\sqrt{5}}{2}$ (the golden ratio). It satisfies $1+\phi = \phi^2$ and $1 < \phi < 2$ (since $1 < 5 < 9 \Rightarrow 1 < \sqrt{5} < 3$), so with induction we get $F_n < \phi^n$ for all $n \in \mathbb{N}$:

- Basis: $F_0 = 0 < 1 = \phi^0$, $F_1 = 1 < \phi = \phi^1$,
- Step: If $F_n < \phi^n$, $F_{n+1} < \phi^{n+1}$, $F_{n+2} = F_{n+1} + F_n < \phi^{n+1} + \phi^n = \phi^{n+2}$. □

Consider the partial sums of the generating function ($N \in \mathbb{Z}_+$):

$(1 - x - x^2)\cdot\sum_{n=0}^{N} F_n\, x^n = F_0\, x^0 + (F_1 - F_0)x^1 + 0 + \ldots - (F_{N-1} + F_N)x^{N+1} - F_N\, x^{N+2}$,

giving, with $x = \frac{1}{2}$, $\sum_{n=0}^{N} 2^{-n}F_n = 2 - 2^{-(N-1)}(F_{N-1} + F_N) - 2^{-N}F_N$. This shows (since $2^{-n}F_n < (\frac{\phi}{2})^n \to 0$ as $n \to \infty$) that $\sum_{n=0}^{N} 2^{-n}F_n \to 2$ as $N \to \infty$.

Answer: The value of the series is 2.

10) We shall (a, 1p) show that x is odd if $x, y \in \mathbb{Z}$ and $y^3 = x^2 + 2$, (b, 2p) show that $R = \mathbb{Z}[\sqrt{2}\,i] = \{a + b\sqrt{2}\,i \mid a, b \in \mathbb{Z}\}$ has unique factorization in ”primes” (apart from the order of factors and factors ±1) and (c, 2p) find all $x, y \in \mathbb{Z}$ with $y^3 = x^2 + 2$.

Solution:

a. If x is even, $x^2 + 2 \equiv_4 2$, but $y^3 \equiv_4 0, 1$ or 3. □

b. Let $\boldsymbol{z, w \in R}$, $\boldsymbol{w \neq 0}$. We shall show that there are $\boldsymbol{q, r \in R}$ with $\boldsymbol{z = wq + r}$, $\boldsymbol{|r|^2 < |w|^2}$, i.e. **division with remainder**, so **the remainder is (strictly) less than the divisor**, as measured by a quantity taking **values in** $\mathbb{N}$ (a well-ordered set).

That is enough to (like in $\mathbb{Z}$, with the Euclidean algorithm, in a finite number of steps) show that there is for all $z, w \in R$ a unique (apart from factors ±1) $\text{sgd}(z, w) = mz + nw$ for some $m, n \in R$.

If you define $p \in R$ to be an ”R-prime” iff it only has divisors ± 1 and $\pm p$, you can show, like in $\mathbb{Z}$ that every $z \in R$ is an (essentially) unique product of ”R-primes”.

(Since $z \mid w \Rightarrow |z|^2 \mid |w|^2$ for $z, w \in \mathbb{C}$, $p = a + b\sqrt{2}\,i$ is an ”R-prime” if $|p|^2 = a^2 + 2b^2$ is an (ordinary) prim, e.g. $1 + \sqrt{2}\,i$, $3 + 4\sqrt{2}\,i$. But ordinary primes are not always ”R-primes”, e.g. $2 = -\sqrt{2}\,i \cdot \sqrt{2}\,i$, $3 = (1 + \sqrt{2}\,i)(1 - \sqrt{2}\,i)$, but 5 is an ”$R$-prime”.)

Now we shall show the result on division with remainder above, so let $z, w \in R$, $w \neq 0$.

Division in $\mathbb{C}$ gives $\frac{z}{w} \in \mathbb{Q}[\sqrt{2}\,i] = \{s + t\sqrt{2}\,i \mid s, t \in \mathbb{Q}\}$ (since $\frac{a + b\sqrt{2}\,i}{c + d\sqrt{2}\,i} = \frac{ac + 2bd}{c^2 + 2d^2} + \frac{bc - ad}{c^2 + 2d^2}\sqrt{2}\,i$).

Take $q = u + v\sqrt{2}\,i$ the number in R closest to $\frac{z}{w}$ ($u \in \mathbb{Z}$ closest to $\frac{ac + 2bd}{c^2 + 2d^2}$ and $v \in \mathbb{Z}$ closest to $\frac{bc - ad}{c^2 + 2d^2}$). Then $|\frac{z}{w} - q|^2 \leq (\frac{1}{2})^2 + (\frac{\sqrt{2}}{2})^2 = \frac{3}{4} < 1$, soo $z = wq + r$ with $r \in R$ and $|r|^2 = |\frac{z}{w} - q|^2 |w|^2 < |w|^2$.

That finishes (the scetch of) the proof of (essentially) unique factorization in R. □

c. We want $x, y \in \mathbb{Z}$ with $y^3 = x^2 + 2 = (x + \sqrt{2}\,i)(x - \sqrt{2}\,i)$ and know that x is odd.

$\text{sgd}(x + \sqrt{2}\,i, x - \sqrt{2}\,i) = d = (\pm)1$, since $\text{sgd}(x + \sqrt{2}\,i, x - \sqrt{2}\,i) = \text{sgd}(x - \sqrt{2}\,i, 2\sqrt{2}\,i)$, so $d \in R$ divides $x + \sqrt{2}\,i$ and $2\sqrt{2}\,i$ and thus $|d|^2 \mid (x^2 + 2)$ and $|d|^2 \mid |2\sqrt{2}|^2 = 8$, but $x^2 + 2$ is odd, so $|d| = 1$. (Or, with the Euclidean algorithm, $(4k \pm 1) - \sqrt{2}\,i = 2\sqrt{2}\,i(-k\sqrt{2}\,i) + (\pm 1 - \sqrt{2}\,i)$; $2\sqrt{2}\,i = (\pm 1 - \sqrt{2}\,i)(-1 \pm \sqrt{2}\,i) \mp 1$.)

That gives $x + \sqrt{2}\,i = (a + b\sqrt{2}\,i)^3$ for some $a, b \in \mathbb{Z}$, since every ”R-prime” p in $x + \sqrt{2}\,i$ is in y, so p^{3k} (some $k \in \mathbb{Z}_+$) is a factor of y^3, thus of $x + \sqrt{2}\,i$ (since it is not in $x - \sqrt{2}\,i$).

$x + \sqrt{2}\,i = (a + b\sqrt{2}\,i)^3$ gives $a(a^2 - 6b^2) = x$ and $b(3a^2 - 2b^2) = 1$. From the second one, $b \mid 1$, so $b = \pm 1$ and $3a^2 - 2 = b = \pm 1$, giving $a^2 = b = 1$ and also $a = \pm 1$, $b = 1$ which gives $x = a(a^2 - 6b^2) = \pm(1 - 6) = \mp 5$. So, at last, $y^3 = x^2 + 2 = 3^3$, $y = 3$.

Answer a,b: See above, c: The only solutions are $\boldsymbol{x = \pm 5}$, $\boldsymbol{y = 3}$.