Matematiska Institutionen
KTH

Exam to the course Discrete Mathematics, SF2736, January 14, 2015, 14.00-19.00.

Observe:

1. Nothing else than pencils, rubber, rulers and papers may be used.
2. Bonus marks from the homeworks will be added to the sum of marks on part I. The maximum number of marks on part I is 15.
3. Grade limits: 13-14 points will give Fx; 15-17 points will give E; 18-21 points will give D; 22-27 points will give C; 28-31 points will give B; 32-36 points will give A.
4. **Observe.** All answers must be justified with a complete argumentation!!

Part I

1. (3p) Find the number of ways to distribute eleven identical yellow balloons and eight identical red balloons to five children. The answer must be given as an integer, or as a product of integers.

   Solution. The number of ways to distribute n identical objects in k labeled boxes is equal to
   $$\binom{n+k-1}{k-1}.$$
   Hence, by multiplication principle, we get that the answer is given by
   $$\binom{11+4}{4} \cdot \binom{8+4}{4} = \frac{11 \cdot 10 \cdot 9 \cdot 8}{1 \cdot 2 \cdot 3 \cdot 4} \cdot \frac{8 \cdot 7 \cdot 6 \cdot 5}{1 \cdot 2 \cdot 3 \cdot 4}$$
   that can be evaluated to
   ANSWER: $330 \cdot 70 = 23100$.

2. (a) (1.5p) Find the greatest common divisor of the integers 518, 434 and 732.

   Solution. The Euclidean algorithm gives
   $$518 = 1 \cdot 434 + 84, \quad 434 = 5 \cdot 84 + 14, \quad 84 = 6 \cdot 14$$
   Hence $\gcd(518, 434) = 14$. As 7 is not a divisor of 732 while 2 are we get
   ANSWER: 2.

   (b) (1.5p) Find the least common multiple of the integers 518, 434 and 732.

   Solution. We start by finding the pairwise greatest common divisors of the given integers:

   $732 = 518{+}214, \quad 518 = 2{\cdot}214{+}90, \quad 214 = 2{\cdot}90{+}34, \quad 90 = 3{\cdot}34{-}12$

   and we can conclude that $\gcd(518, 732) = 2$.
   $$732 = 2 \cdot 434 - 136, \quad 434 = 3 \cdot 136 + 26, \quad 136 = 5 \cdot 26 + 6,$$

from which we get that $\gcd(732, 434) = 2$. Thus

$$732 = a \cdot 2, \quad 518 = b \cdot 7 \cdot 2, \qquad 434 = c \cdot 7 \cdot 2$$

where the integers a, b and c are pairwise coprime. Thus

$$\operatorname{lcm}(732, 518, 434) = abc \cdot 2 \cdot 7 = \frac{(a \cdot 2)(b \cdot 7 \cdot 2)(c \cdot 2 \cdot 7)}{7 \cdot 2 \cdot 2}.$$

Consequently

$$\operatorname{lcm}(732, 518, 434) = \frac{732 \cdot 518 \cdot 434}{7 \cdot 2 \cdot 2} = 5877228.$$

ANSWER: 5877228.

3. (3p) Find and describe a 4-regular graph $\mathcal{G}$ without multiple edges and loops such that $\mathcal{G}$ admits an Euler circuit but no Hamilton cycle.

   (4-regular means that every vertex has degree 4. A loop is an edge the endpoints of which is the same vertex.)

   Solution. We consider the two graphs with vertex sets

   $$E_1 = \{a, a_1, \ldots, a_6\}, \qquad E_2 = \{b, b_1, \ldots, b_6\},$$

   and edges between x_i and x_{i+1}, and x_i and x_{i+2} for $x \in \{a, b\}$, for $i = 1, 2, 3, 4, 5, 6$, (index modulo 6) and with edges between x and x_1 and x_6, for $x \in \{a, b\}$. Then identifying a with b, we get a 4-regular graph with an Euler circuit, as all vertices have an even degree. There are no cycles meeting all vertices, as the vertex $a = b$ must be met twice then.

4. Let $\mathcal{S}_6$ denote the group of all permutations of the elements in the set $\{1, 2, \ldots, 6\}$. Let $\varphi = (1\ \ 6\ \ 2\ \ 5)(4\ \ 5\ \ 2)$ and $\psi = (1\ \ 5)(2\ \ 3)$ be two elements of $\mathcal{S}_6$.

   (a) (1p) Find a permutation γ in $\mathcal{S}_6$ such that $\varphi^2\gamma = \psi$.

   Solution. We start by writing φ as a product of disjoint cycles

   $$\varphi = (1\ \ 6\ \ 2\ \ 5)(4\ \ 5\ \ 2) = (1\ \ 6\ \ 2\ \ 4).$$

   Then

   $$\varphi^2 = (1\ \ 2)(6\ \ 4).$$

   Finally

   $$\gamma = (\varphi^2)^{(-1)}\psi = (1\ \ 2)(6\ \ 4)(1\ \ 5)(2\ \ 3) = (1\ \ 5\ \ 2\ \ 3)(4\ \ 6).$$

   So
   ANSWER: $\gamma = (1\ \ 5\ \ 2\ \ 3)(4\ \ 6)$.

   (b) (1p) Find two distinct permutations δ in $\mathcal{S}_6$ such that $\delta^2 = \psi$.

   Solution. We know that

   $$(a_1\ \ a_2\ \ a_3\ \ a_4)(a_1\ \ a_2\ \ a_3\ \ a_4) = (a_1\ \ a_3)(a_2\ \ a_4).$$

   Thus, with

   $$\delta_1 = (1\ \ 2\ \ 5\ \ 3) \qquad \Longrightarrow \qquad \delta_1^2 = (1\ \ 5)(2\ \ 3)$$

   We know that

   $$(4\ \ 6)(4\ \ 6) = \mathrm{Id}.$$

which implies that with

$$\delta_2 = \delta_1(4\ \ 6)$$

we get $\delta_2^2 = \psi$.
Hence,
ANSWER: For instance $\delta = (1\ \ 2\ \ 5\ \ 3)$ or $\delta = (1\ \ 2\ \ 5\ \ 3)(4\ \ 6)$.

(c) (1p) Is there any permutation β in $\mathcal{S}_6$ such that $\beta^2 = \varphi$.

Solution. We get that

$$\varphi = (1\ \ 6\ \ 2\ \ 4) = (1\ \ 4)(1\ \ 2)(1\ \ 6)$$

is an odd permutation. Thus the given equation cannot have any solution as for any β, the permutation β^2 is an even permutation.

5. (3p) Consider a regular polygon with 12 unlabeled edges. (The polygon can be rotated and flipped.) Find the number of ways to color the edges in q distinct colors.

Solution. We use the lemma of Burnside that tells that the number of colorings is

$$\frac{1}{|G|}\sum_{\varphi\in G}|\mathrm{Fix}(\varphi)|.$$

With the edges labeled 1, 2, ..., 12, where i is a neighbor edge to $i+1$, we get the following table

$\varphi \in G$	$\lvert\mathrm{Fix}(\varphi)\rvert$
$(1)(2)\dots(12)$	q^{12}
$\rho = (1\ \ 2\ \ \cdots\ \ 12)$	q
$\rho^2 = (1\ \ 3\ \ \cdots\ \ 11)(2\ \ 4\ \ \cdots\ \ 12)$	q^2
$\rho^3 = (1\ \ 4\ \ 7\ \ 10)(2\ \ 5\ \ 8\ \ 11)(3\ \ 6\ \ 9\ \ 12)$	q^3
$\rho^4 = (1\ \ 5;\ 9)(2\ \ 6\ \ 10)(3\ \ 7\ \ 10)(4\ \ 8\ \ 12)$	q^4
ρ^5	q
ρ^6	q^6
ρ^7	q
ρ^8	q^4
ρ^9	q^3
ρ^{10}	q^2
ρ^{11}	q
$(1)(2\ \ 12)(3\ \ 11)(4\ \ 10)(5\ \ 9)(6\ \ 8)(7)$	q^7
$(1\ \ 12)(2\ \ 11)(3\ \ 10)(4\ \ 9)(5\ \ 8)(6\ \ 7)$	q^6
dito	q^7
dito	q^6
dito	q^7
dito	q^6
dito	q^7
dito	q^6
dito	q^7
dito	q^6
dito	q^7
dito	q^6

Thus
ANSWER:

$$\frac{1}{24}(q^{12} + 6q^7 + 7q^6 + 2q^4 + 2q^3 + 2q^2 + 4q).$$

Part II

6. The group $G = (Z_{23} \setminus \{0\}, \cdot)$ is a cyclic group.

   (a) (1p) Show that the element 5 generates G.

   Solution. The size of G is $|G| = 22$. Thus the order $\sigma(5)$ of 5 divides 22, that is,
   $$\sigma(5) \in \{1, 2, 11, 22\}.$$
   We note that
   $$5^2 = 2 \neq 1, \qquad 5^{11} = (5^2)^5 5 = 2^5 5 = 9 \cdot 5 = -1 \neq 1.$$
   The only possibility for the order of 5 is that $\sigma(5) = 22$. This fact implies that 5 generates G.

   (b) (2p) Find another element of G that generates G.

   Solution. We consider the element $g = 5^3$. Then, as order of 5 is 22,
   $$g^2 = (5^3)^2 = 5^6 \neq 1, \qquad g^{11} = (5^3)^{11} = 5^{22}5^{11} = -1 \neq 1,$$
   Consequently $\sigma(g) \notin \{1, 2, 11\}$ so $\sigma(g) = 22$. Thus g generates G.
   ANSWER: For example, 5^3, that is, 10.

7. (4p) Find the number of equivalence relations $\mathcal{R}$ on a set $M = \{1, \ldots, 9\}$ such that $|\mathcal{R}| = 27$ and
   $$|\{x \in M \mid 1\mathcal{R}x\}| = |\{x \in M \mid 2\mathcal{R}x\}| = |\{x \in M \mid 3\mathcal{R}x\}| = 3.$$

   Solution. We consider distinct cases depending on whether or not $1 \sim 2$, $1 \sim 3$ or $2 \sim 3$, respectively.

   Case 1. None of 1, 2 or 3 are equivalent. We know that each of the sets above are equivalence classes that are either disjoint or equal. Thus, in this case
   $$\{x \in M \mid 1\mathcal{R}x\} \cup \{x \in M \mid 2\mathcal{R}x\} \cup \{x \in M \mid 3\mathcal{R}x\} = \{1 \ldots, 9\}.$$
   As $\mathcal{R}$ is an equivalence relation we know that for any equivalence class C_a,
   $$x, y \in C_a \qquad \Longleftrightarrow \qquad x \sim y.$$
   Thus every equivalence class of size k contributes with k^2 elements (x, y) to $\mathcal{R}$. So in this case $\mathcal{R}$ has size $3^2 + 3^2 + 3^2 = 27$.

   An equivalence relation is defined by its equivalence classes. These are in this case three labeled sets, with one element already destinated to the equivalence class. Thus the number of equivalence relations in this case is
   $$\binom{6}{2, 2, 2} = \frac{6!}{2 \cdot 2 \cdot 2} = \frac{720}{8} = 90.$$

   Case 2. $1 \sim 2$ but 1 is not equivalent to 3. In this case six of the elements are distributed to $C_1 = C_2$ and C_3, each contributing with 9 elements to $\mathcal{R}$. Remains three elements to be distributed to equivalence classes such that these equivalence classes contributes with $27 - 2 \cdot 9$ elements to $\mathcal{R}$. The only possibility is that they constitute an equivalence class of their

own. With arguments as above we get that the number of equivalence classes in this case is

$$\binom{6}{1,2,3} = \frac{6!}{1 \cdot 2 \cdot 3} = \frac{720}{12} = 60.$$

Case 3. $1 \sim 3$ but 1 is not equivalent to 2. As above we get 60 distinct equivalence relations.

Case 4. $3 \sim 2$ but 1 is not equivalent to 3. As above we get 60 distinct equivalence relations.

Case 5. $1 \sim 2 \sim 3$. The remaining six elements $\{4, \ldots, 6\}$ shall be partitioned into equivalence classes such that the sum of contributions from these equivalence classes to $\mathcal{R}$ is $27 - 9 = 18$. There are two possibilities three equivalence classes of size 4, 1 and 1, respectively, or two equivalence classes both of size 3. The number of possibilities in this case are thus

$$\binom{6}{4} + \frac{1}{2}\binom{6}{3,3} = 15 + 10 = 25.$$

We sum over all possibilities and get the

ANSWER: $90 + 3 \cdot 60 + 35 = 295$.

8. (4p) Let G be a graph with vertex set V and edge set E, with no multiple edges and no loops (a loop is an edge the endpoints of which is one single vertex). Assume that the lengths of the cycles belong to the set $\{8, 10, 12, 14\}$ and that

$$\{\delta(v) \mid v \in V\} = \{9, 11, 13, 15, 17\},$$

where $\delta(v)$ denotes the valency (degree) of the vertex v. Show that, for every integer q in the interval $19 \leq q \leq 72$, the edges can be colored in exactly q distinct colors such that no two edges of the same color meet at a vertex. (The number of possibilities for q can certainly be proved to be larger than this interval, but to get 4p it is enough to verify the given interval of possibilities.)

Solution. As all cycles have an even length, we get from a known theorem that the graph is bipartite with vertex set $X \cup Y$ with no edges between vertices in X and no edges between vertices in Y. As the max-degree is 17 there is, by another known theorem, an edge coloring in 17 distinct colors $c_1, \ldots, c_{17}$. If we can prove that the graph has at least 72 edges, we can take away 17 edges colored in the colors $c_1, \ldots, c_{17}$ and give $q-17$ of the remaining edges the $q-17$ distinct (new) colors $d_1, \ldots, d_{q-17}$, where

$$\{c_1, \ldots, c_{17}\} \cap \{d_1, \ldots, d_{q-17}\} = \emptyset.$$

We now prove that fact. One of the vertices v has degree 17. Assume that v belongs to the set of edges X. Then all neighbors of v belong to Y and thus $|Y| \geq 17$. All vertices of Y has a degree larger than 8. Thus the number of edges is at least equal to $17 \cdot 9 = 153$.

Part III

9. Let as usual $\mathcal{S}_n$ denote the group consisting of all permutations of the elements in the set $\{1, 2, \ldots, n\}$.

   (a) (1p) Does an equation $\psi^2 = \varphi$ have a solution ψ for any even permutation φ.

   Solution. No. Every permutation ψ can be expressed as a product of disjoint cycles:

   $$\psi = c_1 c_2 \cdots c_k,$$

   and for disjoint cycles

   $$\psi^2 = c_1^2 c_2^2 \cdots c_k^2.$$

   The square of a cycle c_i of an odd length is a cycle of the same length, the square of an cycle of an even length is a product of two cycles of half length:

   $$\begin{array}{rcl} (a_1 a_2 \ldots a_{2k+1})(a_1 a_2 \ldots a_{2k+1}) & = & (a_1 a_3 \ldots a_{2k+1} a_2 a_4 \ldots a_{2k}) \\ (a_1 a_2 \ldots a_{2k})(a_1 a_2 \ldots a_{2k}) & = & (a_1 a_3 \ldots a_{2k-1})(a_2 a_4 \ldots a_{2k}) \end{array} \tag{1}$$

   The permutation

   $$\varphi = (1\ \ 2)(3\ \ 4\ \ 5\ \ 6)$$

   is an even permutation, as φ is a product of an even number of 2-cycles:

   $$\varphi = (1\ \ 2)(3\ \ 6)(3\ \ 5)(3\ \ 4).$$

   and, from Equation (1) we get that no permutation ψ can satisfy the equation $\psi^2 = \varphi$ as φ is expressed as just two disjoint cycles which are of distinct lengths.

   (b) (1p) Derive a formula for the number of solutions ψ in $\mathcal{S}_n$ to the equation $\psi^4 = \mathrm{Id}$.?

   Solution. With

   $$\psi = c_1 c_2 \cdots c_k,$$

   as a product of disjoint cycles we have

   $$\psi^4 = c_1^4 c_2^4 \cdots c_k^4.$$

   If $c_i^4 = \mathrm{Id}$. then the length of the cycle c_i is either 1, 2 or 4. Thus we shall sum over all possibilities to split the set $\{1, 2, \ldots, n\}$ into mutually disjoint unlabeled subsets of size 1, 2 and 4. Note that for a given subset $\{a_1, a_2, a_3, a_4\}$ there are 6 possibilities to form a 4-cycle:

   $$(a_1\ \ a_2\ \ a_3\ \ a_4), \quad (a_1\ \ a_2\ \ a_4\ \ a_3), \quad \ldots, \quad (a_1\ \ a_4\ \ a_3\ \ a_2).$$

   Thus we get the formula

   $$\sum \frac{6^i}{i!j!k!} \binom{n}{4, \ldots 4, 2 \ldots 2, 1 \ldots 1}$$

   where in the multinomial coefficient the number of 4:s is equal to i, the number of 2:s is equal to j and the number of 1:s is equal to k, and the summation is over all non-negative integers such that $4i + 2j + k = n$.

(c) (3p) Can the number of solutions ψ in $\mathcal{S}_n$ to an equation $\psi^2 = \varphi$, where $\varphi \neq \mathrm{Id.}$, be larger than the number of solutions in $\mathcal{S}_n$ to the equation $\psi^2 = \mathrm{Id.}$.

Solution. Consider φ as a product of disjoint cycles:

$$\varphi = d_1 d_2 \cdots d_k.$$

From Equation (1) we get that a solution ψ to $\psi^2 = \varphi$ can be obtained by combining pairs of two cycles of the same length to cycles of double length, or for a cycle d of odd length obtain, using Equation (1), one cycle of the same length, the square of which is equal to d. Thus the number of solutions ψ to the equation $\psi^2 = \varphi$ is less than the number of ways N_k to find a partition of the set $\{1, 2, \ldots, k\}$ (the index set of cycles of φ) into unlabeled sets of size 2 or 1. Trivially N_k is an strictly increasing function in k, that is,

$$k < n \qquad \Longrightarrow \qquad N_k < N_n.$$

Similarly to the solution of previous subproblem, we get that the number of solutions to $\psi^2 = \mathrm{Id.}$ is equal to N_n. If $\varphi \neq \mathrm{Id.}$ we have that $k < n$. Thus the answer is
ANSWER: No

10. (5p) Evaluate the new idea below for the construction of an 1-error-correcting binary code C. Discuss whether the construction is fruitful, give its advantages and disadvantages in comparison with the traditional Hamming construction of 1-error-correcting codes.

Idea. Use a binary $k \times n$-matrix $\mathbf{H}$ and two distinct $k \times 1$-matrices $\mathbf{b}_1$ and $\mathbf{b}_2$ to define a code C by

$$C = \{\mathbf{c} = (c_1 \ \ldots \ c_n) \mid \mathbf{H}\mathbf{c}^T = \mathbf{b}_1\} \cup \{\mathbf{c} = (c_1 \ \ldots \ c_n) \mid \mathbf{H}\mathbf{c}^T = \mathbf{b}_2\}.$$

Also discuss further possible generalizations of this construction.

Solution. We first show that, under some circumstances, the construction produces a 1-error-correcting code. Let

$$\mathbf{b} = \mathbf{b_2} - \mathbf{b_1},$$

and let L be a subgroup of Z_2^k not containing the element $\mathbf{b}$. Use the non-zero elements of L as columns in H. Then $n = |L| - 1$, so the length of the code is $n = |L| - 1$. Let, for $i = 1, 2$,

$$C_i = \{\mathbf{c} = (c_1 \ \ldots \ c_n) \mid \mathbf{H}\mathbf{c}^T = \mathbf{b}_i\}.$$

We now prove that the minimum distance in C_1 and C_2 is three. Assume $\mathbf{c} \in C_i$. Changing one coordinate position in $\mathbf{c}$, the position i, to the word $\mathbf{c}'$ will give

$$\mathbf{H}\mathbf{c}'^T = \mathbf{b_1} + \mathbf{k}_i,$$

where $\mathbf{k}_i$ is the i:th column of $\mathbf{H}$, which is neither equal to $\mathbf{b}_1$ nor $\mathbf{b}_2$ as $\mathbf{k}_i$ neither is equal to $\mathbf{0}$ nor $\mathbf{b}$. Similar arguments show that the distance between words of C_1 and C_2 is at least equal to three. Thus the code obtained in this way is 1-error-correcting.

For the purpose of evaluating the construction we start by calculating the number of words of the code C. Let $\mathbf{c}_i$ be a word such that $\mathbf{H}\mathbf{c}_i^T = \mathbf{b}_i$, for $i = 1, 2$. Then C_i is the coset

$$C_i = \mathbf{c}_i + \{\mathbf{c} \mid \mathbf{H}\mathbf{c}^T = \mathbf{0}\}.$$

Thus

$$|C_i| = |\{\bar{c} \mid \mathbf{H}\mathbf{c}^T = \mathbf{0}\}| = 2^{n-k} = 2^{|L|-1-k}.$$

As L is a non-trivial subgroup of Z_2^k, the maximum size of L is

$$|L| \leq 2^{k-1}.$$

Thus the maximum size of the code is

$$|C_1 \cup C_2| \leq 2 \cdot 2^{n-k} = 2 \cdot 2^{2^{k-1}-1-k} = 2^{2^{k-1}-1-(k-1)}$$

which is he number of words of an ordinary Hamming code of length $m = 2^{k-1} - 1$.

An disadvantage with this construction is the error-correcting procedure. In the traditional Hamming construction you multiply the received word with $\mathbf{H}$. The column $\mathbf{k}$ so obtained indicates the position where the error occurred. With the new construction you must check which column in $\mathbf{H}$ is equal to one of the columns $\mathbf{k} - \mathbf{b}_1$ or $\mathbf{k} - \mathbf{b}_2$.

A possible advantage could be if we obtained a new code. However the new code is just a coset of a linear code. To see this assume that $\mathbf{b}_1 = \mathbf{0}$. Then C_1 is, as being a null space of a matrix, a linear code. Furthermore, if $\mathbf{c}$ and $\mathbf{c}'$ are two elements of C_2, that is,

$$\mathbf{H}\mathbf{c}^T = \mathbf{b}, \qquad \mathbf{H}\mathbf{c}'^T = \mathbf{b},$$

then

$$\mathbf{H}(\mathbf{c}^T + \mathbf{c}'^T) = \mathbf{b} + \mathbf{b} = \mathbf{0}$$

Thus $\mathbf{c} + \mathbf{c}'$ belongs to C_1, which implies that $C = C_1 \cup C_2$ is linear. Now let $\mathbf{b}_1$ be any word and let $\bar{d}$ be a word such that

$$\mathbf{H}\mathbf{d}^T = \mathbf{b}_1.$$

Then, for $\mathbf{c}$ in the above defined code C

$$\mathbf{H}(\mathbf{d} + \mathbf{c})^T = \mathbf{b}_i$$

depending on whether $\bar{c}$ belongs to C_1 or C_2.

A generalization could be to let C be a suitable union

$$\bigcup_{i=1}^{t} (\{\mathbf{c} = (c_1 \ \ldots \ c_n) \mid \mathbf{H}\mathbf{c}^T = \mathbf{b}_i\}).$$

With suitable sets of columns of $\mathbf{H}$, the non-zero elements of a subgroup L of Z_2^k, we will, with the same arguments as above, obtain an 1-error-correcting code by considering a partition of Z_2^k into cosets of L. The error-correcting procedure will be even worse than for the original idea for a new construction of 1-error-correcting code.