Matematiska Institutionen
KTH

Solutions to the exam to the course Discrete Mathematics, SF2736, December 19, 2011.

Observe:

1. You are not allowed to use anything else than pencils, rubber, rulers and papers at this exam.
2. To get the maximum number of points on a problem it is not sufficient to just give an answer, you must also provide explanations.
3. Bonus points from the homeworks will be added to the sum of the points on part I.
4. Grade limits: 13-14 points will give an Fx; 15-17 points will give an E; 18-21 points will give a D; 22-27 points will give a C; 28-31 points will give a B; 32-36 points will give an A.

Part I

1. (3p) Draw a bipartite graph with 8 vertices and 12 edges that has an Euler circuit but no Hamiltonian cycle and draw another bipartite graph, also with 8 vertices and 12 edges, that has an Hamiltonian cycle but no Euler circuit.

   Solution: The complete bipartite graph $K_{2,6}$ has no Hamilton cycle, but as all vertices have an even degree, this graph has an Euler circuit.

   Consider the complete bipartite graph $K_{4,4}$. The graph has a complete matching, the set of edges

   $$\{(x_1, y_1), (x_2, y_2), (x_3, y_3), (x_4, y_4)\},$$

   (where the vertices in the different parts of the bipartite graph have the evident notation). Delete the edges in the complete matching above and consider the resulting graph that has 12 edges. Now, as there are vertices of odd degree (in fact all vertices) there is no Euler circuit. The following cycle will be a Hamiltonian cycle

   $$x_1y_2x_3y_4x_2y_1x_4y_3x_1$$

2. (3p) Use the technique with generating functions to find all sequences $a_0, a_1, a_2, \ldots$ that satisfy the recursion

$$a_{n+2} = 7a_{n+1} - 10a_n \qquad \text{for} \qquad n = 0, 1, 2, \ldots \ .$$

Solution: Let

$$A(t) = a_0 + a_1 t + a_2 t^2 + \ldots$$

We multiply the given equality with t^{n+2}, for $n = 0, 1, 2, \ldots$, and sum. We then get the equality

$$A(t) - a_1 t - a_0 = 7t(A(t) - a_0) - 10A(t).$$

Simplifying we get

$$A(t) = \frac{(a_1 - 7a_0)t + a_0}{1 - 7t + 10t^2}$$

We factorize the denominator, make partial fractions and sum a geometric series

$$A(t) = \frac{(a_1 - 7a_0)t - a_0}{(1-2t)(1-5t)} = \frac{A}{1-2t} + \frac{B}{1-5t} = A \cdot \sum_{n=0}^{\infty} (2t)^n + B \cdot \sum_{n=0}^{\infty} (5t)^n$$

for some real numbers A and B. So

ANSWER: $a_n = A \cdot 2^n + B \cdot 5^n$ for $n = 0, 1, 2, \ldots$.

3. (3p) John will, as a Christmas present, get a package with ten bolls. They are colored either green, red, yellow or blue. How many possible distinct packages are there, if a package must contain at least one ball of each color? The solution shall, besides explanations, also contain an answer, to the question, given as an integer.

Solution: An equivalent problem is to place 10 identical balls into 4 paint pots with the four given colors, in such a way that each pot will contain at least one ball. The formula for the number of ways this can be done is

$$\binom{10 - 4 + 3}{3} = \frac{9 \cdot 8 \cdot 7}{1 \cdot 2 \cdot 3} = 84.$$

4. (3p) Find the least positive remainder when 37^{121} is divided by 42.

Solution: As 42 has the prime factorization

$$42 = 2 \cdot 3 \cdot 7$$

we get that for the Euler φ-function

$$\varphi(42) = 42(1 - \frac{1}{2})(1 - \frac{1}{3})(1 - \frac{1}{7}) = 12.$$

As

$$37^{\varphi(42)} \equiv 1 \pmod{42},$$

we may then conclude that

$$37^{121} \equiv_{42} (37^{12})^{10} \cdot 37 \equiv_{42} 1^{10} \cdot 37 = 37.$$

5. (3p) Find the smallest subgroup H of the group $G = (Z_{30}, +)$ with the property that both 3 and 8 belongs to the same coset of H in G.

   Solution: There are elements a in G, and h and h' in H such that

   $$3 = a + h \qquad \text{and} \qquad 8 = a + h'.$$

   Subtraction gives that

   $$5 = 8 - 3 = (a + h') - (a + h) = h' - h$$

   which thus has to be an element in H, as $h' - h \in H$. The smallest subgroup that contains the element 5 is the cyclic subgroup of G generated by 5. The answer is thus given by

   $$H = \langle 5 \rangle = \{5, 10, 15, 20, 25, 0\}.$$

Part II

6. (3p) A tree is a connected graph without any cycles. A forest is a graph that consists of trees. Find the least number of trees, as well as the largest number of trees, in a forest with 100 vertices if at least 27 of the vertices has degree 3.

   Solution: The forest can contain just one tree. Put together 27 vertices of degree 3 as shown below:

   $$\perp\perp\perp \ldots \perp$$

   This subgraph will contain 82 vertices. So remains 18 vertices. Just make a path of these vertices and attach to the subgraph above and you get a tree with 100 vertices.

   Assume the number of trees in a forest is t, and the trees are T_1, T_2, ..., T_t, each with v_i vertices, and thus with $e_i = v_i - 1$ edges. As given is that

   $$v_1 + v_2 + \ldots + v_t = 100$$

   we get, using the fact that $e_i = v_i - 1$, that

   $$t + e_1 + e_2 + \ldots + e_t = 100,$$

   that is, the number of trees is

   $$t = 100 - |E|,$$

   where $|E|$ is the number of edges in the forest. So we try to find the minimum number of edges in an acyclic graph where at least 27 of the vertices have degree 3.

   As the sum of all degrees is twice the number of edges

   $$\sum_{v \in V} \delta(v) = 2|E| \tag{1}$$

   we immediately get the fewest number of edges, (or the largest number of trees), when we have as few vertices as possible of degree one and two. So now some reasoning.

Every tree has leaves. A tree with four vertices of which one has degree 3 has three leaves. If we add two brances to one of the leaves, we get a tree with two vertices of degree 3 and four leaves. So the number of leaves add by one, every time we let a tree grow in this way. This gives a contribution of 1 to the sum in the Equation (1), except for the addition of 3 from the vertex of degree 3. If we just add one new branch to a leaf, we have the same number of leaves but we get a vertex of degree 2, which add 2 to the sum in the Equation (1). So for each tree, the most "economical" procedure, economical in the sense of using as few edges as possible, is to add two branches to every leaf when growing. In this way, a tree with k vertices of degree 3 will get $2 + k$ leaves.

The conclusion is that the optimal situation appears when we let one tree be constructed as described above and containing all 27 vertices of degree 3 and containing 29 leaves. The number of vertices in this tree will be $27 + 29 = 56$. It remains 44 vertices. So the answer will be

Answer: There can be one tree, and not more than 45 trees in the forest.

7. (4p) Find the number of equivalence relations on the set $A = \{1, 2, 3, 4, 5, 6, 7\}$ such that 1 and 2 are not equivalent, 2 and 3 are not equivalent, 3 and 4 are not equivalent. The solution shall, besides explanations, also contain an answer, to the question, given as an integer.

Solution: There is a one to one correspondence between the set of equivalence relations on a set M and the family of all partitions of M, the corresponding partition is the set of equivalence classes associated to the equivalence relation.

The number of ways to partition a set with n elements into k non empty subsets is given by the Stirling number $S(n, k)$, which can recursively be derived by the formula

$$S(n, k) = S(n - 1, k - 1) + k \cdot S(n - 1, k).$$

The total number N of equivalence relations on a set with 7 elements will thus be

$$S(7, 1) + S(7, 2) + S(7, 3) + \ldots + S(7, 7).$$

We will use the principle of inclusion exclusion to solve the actual problem. Let A denote the set of equivalence relations where 1 and 2 are equivalent, B the equivalence relations where 2 and 3 are equivalent and C the equivalence relations where 3 and 4 are equivalent.

When two elements are equivalent, they will belong to the same equivalence class, and thus in this context they can be regarded as the same element. Hence,

$$|A| = S(6, 1) + S(6, 2) + S(6, 3) + \ldots + S(6, 6) = |B| = |C|.$$

If 1 and 2 are equivalent and 2 and 3 are equivalent then, by the transitivity property of equivalence relations, also 1 and 3 are equivalent, and similarly for 3 and 4. We thus get

$$|A \cap B| = S(5, 1) + S(5, 2) + S(5, 3) + S(5, 4) + S(5, 5) = |B \cap C|,$$

and

$$|A \cap B \cap C| = S(4,1) + S(4,2) + S(4,3) + S(4,4).$$

Similarly

$$|A \cap C| = S(5,1) + S(5,2) + S(5,3) + S(5,4) + S(5,5).$$

We need a lot of Stirling numbers, so lets do the recursively derivation of them, using the formula above.

$$S(n,1) = 1 \qquad \text{and} \qquad S(n,n) = 1$$

so

$$S(3,2) = 3, \quad S(4,2) = 7, \quad S(4,3) = 6.$$

And further on:

$$S(5,2) = 15, \quad S(5,3) = 25, \quad S(5,4) = 10,$$

$$S(6,2) = 31, \quad S(6,3) = 90, \quad S(6,4) = 65, \quad S(6,5) = 15$$

$$S(7,2) = 63, \quad S(7,3) = 301, \quad S(7,4) = 350, \quad S(7,5) = 140, \quad S(7,6) = 21.$$

So summing these numbers we get

$$N = 877,\ |A| = |B| = |C| = 203,\ |A \cap B| = |A \cap C| = |B \cap C| = 52,\ |A \cap B \cap C| = 15.$$

The principle of inclusion exclusion finally gives the following answer

ANSWER: $877 - 3 \cdot 203 + 3 \cdot 52 - 15 = 409$.

8. Let $\mathcal{S}_n$ denote the group that consists of all permutations of the elements in the set $\{1, 2, 3, \ldots, n\}$.

   (a) (1p) Find all cyclic subgroups of order 4 in $\mathcal{S}_4$.

   Solution: A cyclic group of order 4 must be generated by a 4-cycle. There are six 4-cycles in $\mathcal{S}_4$:

   $$(1\ 2\ 3\ 4), \quad (1\ 2\ 4\ 3), \quad (1\ 3\ 2\ 4), \quad (1\ 3\ 4\ 2), \quad (1\ 4\ 2\ 3), \quad (1\ 4\ 3\ 2).$$

   We let these elements generate subgroups. In fact we get three different cyclic subgroups of order 4:

   $$\langle (1\ 2\ 3\ 4) \rangle = \{(1\ 2\ 3\ 4), (1\ 3)(2\ 4), (1\ 4\ 3\ 2), \mathrm{id}\}$$

   $$\langle (1\ 2\ 4\ 3) \rangle = \{(1\ 2\ 4\ 3), (1\ 4)(2\ 3), (1\ 3\ 4\ 2), \mathrm{id}\}$$

   $$\langle (1\ 3\ 2\ 4) \rangle = \{(1\ 3\ 2\ 4), (1\ 2)(3\ 4), (1\ 4\ 2\ 3), \mathrm{id}\}$$

   (b) (1p) Find the number of cyclic subgroups of order 4 in $\mathcal{S}_n$, for $n \geq 4$.

   Solution: A cyclic subgroup of order 4 is generated by a permutation that consists of at least one 4-cycle together with a number of 2-cycles. We first derive a formula for the number of permutations that consists of $i \geq 1$ 4-cycles and j 2-cycles. Then we sum over all such possible cases.

The number of ways to find elements to the 4-cycles and 2-cycles is

$$P_{i,j} = \binom{n}{4,4,\ldots,4,2,2,\ldots,2,n-4i-2j} = \frac{1}{i!}\cdot\frac{1}{j!}\cdot\frac{n!}{(4!)^i(2!)^j(n-4i-2j)!}$$

as the cycles in the permutation are not labeled.
Given any four elements, you can form $3! = 6$ distinct 4-cycles from them. So the number of permutations of order 4 will be

$$(3!)^i \cdot P_{ij}.$$

As every cyclic subgroup

$$H = \langle\varphi\rangle = \{\varphi, \varphi^2, \varphi^3, \mathrm{id.}\}$$

of order four contains exactly two elements of order four, the elements φ and φ^3, and every element of order four is in a unique cyclic subgroup of order four, we must divide the total number of elements of order four by two to get the number of cyclic subgroups of order four. Hence
ANSWER:

$$\frac{1}{2}\sum_{4i+2j\leq n, i\geq 1, j\geq 0}\frac{1}{i!j!}\cdot\frac{n!}{4^i 2^j(n-4i-2j)!}$$

(c) (2p) Give a formula for the number of cyclic subgroups of order p in $\mathcal{S}_n$, for every prime number $p \leq n$.

Solution: The order of an element in a group G always divides the size $|G|$ of G. Hence, every element $\varphi \neq \mathrm{id.}$ in a cyclic group of order p, where p is a prime, must have oder p and, again as p is a prime, must be a p-cycle or a product of p-cycles. Furthermore, we may conclude every cyclic subgroup of order p will contain $p-1$ distinct elements of order p. We also note that

$$\psi \in \langle\varphi\rangle \qquad \Longrightarrow \qquad \langle\psi\rangle = \langle\varphi\rangle \tag{2}$$

for any two elements φ and ψ of the same cyclic subgroup of order p.
The number of distinct p-cycles you can form by using the elements in the set $\{x_1, x_2, \ldots, x_p\}$ is $(p-1)!$. Hence the number of elements of order p in $\mathcal{S}_n$ will be

$$\sum_{i=1}^{\lfloor n/p\rfloor}\frac{1}{i!(n-pi)!}\cdot\binom{n}{p,p,\ldots,p,1,1,\ldots,1}((p-1)!)^i = \sum_{i=1}^{\lfloor n/p\rfloor}\frac{1}{i!(n-pi)!}\cdot\frac{n!}{p^i}$$

And these are, by the equation above, to be distributed among the subgroups of order p, each containing $p-1$ distinct elements of order p.
Hence,
ANSWER:

$$\frac{1}{p-1}\cdot\sum_{i=1}^{\lfloor n/p\rfloor}\frac{1}{i!(n-pi)!}\cdot\frac{n!}{p^i}$$

Part III

9. For an 1-error correcting code C of length n we will below denote the set of words that C cannot correct by $D(C)$, i.e., $D(C)$ denotes the set of words at distance at least two from each of the words in C.

   (a) (1p) The 1-error correcting code C is linear and the matrix $\mathbf{H}$ below is a parity check matrix for C:

   $$\mathbf{H} = \begin{bmatrix} 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

   Show that the set of words $D(C)$ is a 1-error correcting code that is not linear.

   Solution: Let $\bar{x} = (x_1, x_2, \ldots, x_6)$. If $\mathbf{H}\bar{x}^T = \bar{0}^T$ then $\bar{x} \in C$. If $\mathbf{H}\bar{\mathbf{x}}^{\mathbf{T}}$ is equal to one of the six columns in $\mathbf{H}$ then $\bar{x}$ is a word that can be corrected. There is exactly one further outcome of the multiplication of $\mathbf{H}$ with a word, as there in total are just seven nonzero columns of "height" 3, namely

   $$\mathbf{H}\bar{x}^T = \bar{c}^T \tag{3}$$

   where $\bar{c} = (0, 0, 1)$, which is the only word of length 3 that does not appear as a column in $\mathbf{H}$.

   Let $\bar{x}_p$ be a solution to the Equation (3), for example $\bar{x}_p = (1, 0, 0, 1, 0, 0)$. Then, form the theory of elementary linear algebra, we know that every other solution $\bar{x}$ is given by

   $$\bar{x} = \bar{x}_p + \bar{x}_h$$

   where $\bar{x}_h$ is a solution to the corresponding homogenious system, that is, $\bar{x}_h \in C$, and furthermore, any word on this form will be a solution.

   We now show that the minimum distance in this set is three. Take any two words $\bar{x} = \bar{x}_p + \bar{x}_h$ and $\bar{x}' = \bar{x}_p + \bar{x}'_h$ in this set. The distance is equal to the number of ones in the word $\bar{x} - \bar{x}'$. As

   $$\bar{x} - \bar{x}' = (\bar{x}_p + \bar{x}_h) - (\bar{x}_p - \bar{x}'_h) = \bar{x}_h - \bar{x}'_h \in C$$

   as C is a linear code, and no words of C, except the all zero word, contain fewer that 3 ones, the distance between $\bar{x}$ and $\bar{x}'$ must be at least 3.

   We have thus proved that the minimum distance in the set of words that C cannot correct is three. This fact means that this set will constitute a 1-error correcting code.

   (b) (2p) Show that, for every linear 1-error correcting code C of length n and size $|C| = 2^{n-m}$ with a parity check matrix $\mathbf{H}$ with m rows and $n = 2^m - 2$ columns, the set of words $D(C)$ is a 1-error correcting code that is not linear.

   Solution: There are in total 2^m distinct columns of "height" m, of which one is the zero columns, and $2^m - 2$ appear in the matrix $\mathbf{H}$. Let $\bar{c}^T$ be the remaining column. So the words that C cannot correct are those that satisfy an equation similar to the Equation (3). The rest of the motivation is the same as above.

(c) (2p) Can the statement above be true if the matrix $\mathbf{H}$ has m rows and $n = 2^m - 3$ columns? Always, under certain conditions, or never?

Solution: Never is the answer. Let $\bar{c}^T$ and $\bar{c}'^T$ be the two nonzero columns that do not appear as columns in $\mathbf{H}$. Then a word $\bar{x}$ cannot be corrected if and only if

$$\mathbf{H}\bar{x}^T \in \{\bar{c}^T, \bar{c}'^T\}.$$

Let $\bar{k}^T = \bar{c}^T + \bar{c}'^T$, which must be a column of $\mathbf{H}$, as it is nonzero and distinct from both $\bar{c}^T$ and $\bar{c}'^T$.

Let the ith column of $\mathbf{H}$ be $\bar{k}_i^T$. Assume that $\bar{k}_{i_0}^T$ is distinct from $\bar{k}^T$ and

$$\bar{k}_j^T = \bar{k}_{i_0}^T + \bar{c}^T \qquad \text{and} \qquad \bar{k}_{j'}^T = \bar{k}_{i_0}^T + \bar{c}'^T,$$

or equivalently

$$\bar{k}_j^T + \bar{k}_{i_0}^T = \bar{c}^T \qquad \text{and} \qquad \bar{k}_{j'}^T + \bar{k}_{i_0}^T = \bar{c}'^T.$$

So there are two words, each with just two ones, the ones in the positions j and i_0 and the ones in the positions j' and i_0, that belong to the set of words that cannot be corrected. The distance between these words is just two. They differ in the positions j and j'. The minimum distance is thus 2, and the code is not 1-error correcting.

10. Let G be a finite group and a and b two elements in G such that $ab = ba$. Let $\sigma(g)$ denote the order of an element g in G.

(a) (2p) Show that if $\gcd(\sigma(a), \sigma(b)) = 1$ then $\sigma(ab) = \text{lcm}(\sigma(a), \sigma(b))$.

Solution: We first show that the cyclic groups generated by a and b have a trivial intersection. It is well known that the intersection of any two subgroups of a group G is a subgroup of G. Let

$$H = \langle a \rangle \cap \langle b \rangle.$$

Then by the theorem of Langrange $|H|$ divides $|\langle a \rangle| = \sigma(a)$, and similarly $|H|$ divides $\sigma(b)$. As $\gcd(\sigma(a), \sigma(b)) = 1$ the only possibility is that $|H| = 1$.

Let $n = \sigma(ab)$, then, as $ab = ba$, we get that $a^n b^n = e$. If $a^n \neq e$ then $a^n = (b^n)^{-1}$ which is an element in both $\langle a \rangle$ and $\langle b \rangle$ and hence $a^n \in H$. This means that $a^n = e$. Similarly $b^n = e$.

We now show that this implies that $\sigma(a)$ divides n, and similarly for b.

If $n = k \cdot \sigma(a) + r$, where $0 \leq r < \sigma(a)$, then

$$e = a^n = (a^{\sigma(a)})^k \cdot a^r = e^k \cdot a^r = a^r,$$

which contradicts the fact that $\sigma(a)$ is the smallest integer t such that $a^t = e$, unless $r = 0$. Thus, $\sigma(a)$ divides n.

We now know that both $\sigma(a)$ and $\sigma(b)$ divides n. By definition, this means that $\text{lcm}(\sigma(a), \sigma(b))$ divides n.

As the orders of a and b are relatively prime, the least common multiple of the orders of a and b is the product of the orders. Hence,

$$(ab)^{\mathrm{lcm}(\sigma(a),\sigma(b))} = (ab)^{\sigma(a)\sigma(b)} = (a^{\sigma(a)})^{\sigma(b)} \cdot (b^{\sigma(b)})^{\sigma(a)} = e.$$

To summarize: We have proved that $\mathrm{lcm}(\sigma(a), \sigma(b))$ divides the order of ab, and that $(ab)^{\mathrm{lcm}(\sigma(a),\sigma(b))} = e$. This means that the order of ab is as stated in the problem.

(b) (3p) Can $\sigma(ab) = \mathrm{lcm}(\sigma(a), \sigma(b))$ if $\gcd(\sigma(a), \sigma(b)) \neq 1$? Always, under certain conditions, or never? (A correct guess will give 1p.)

Solution: The correct answer is "under certain conditions". We give two examples.

Let $G_1 = (Z_2, +) \times (Z_4, +)$. If $a = (1, 0)$ and $b = (0, 1)$ then $a + b = (1, 1)$. We get

$$(1,1) \neq (0,0), \quad 2 \cdot (1,1) = (0,2) \neq (0,0), \quad 3 \cdot (1,1) = (1,3) \neq (0,0),$$

and as further $4 \cdot (1, 1) = (0, 0)$, we get that

$$\sigma(a + b) = 4 = \mathrm{lcm}(\sigma(a), \sigma(b)).$$

Let $G_2 = (Z_2, +)$ and let $a = b = 1$. Then $a + b = 0$ and

$$\sigma(a + b) = 1 \neq 2 = \mathrm{lcm}(\sigma(a), \sigma(b)).$$