Matematiska Institutionen
KTH

Solutions to the exam to the course Discrete Mathematics, SF2736, 08.00 to 13.00 on June 7, 2011.

Observe:

1. Nothing else than pencils, rubber, rulers and papers may be used.
2. Bonus points from the homeworks will be added to the sum of points on part I.
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.

Part I

1. (3p) Find the least positive remainder when 7^{1024} is divided by 31.

   Solution: We will use the theorem of Fermat, that is, if p is a prime number that does not divide the integer a, then

   $$a^{p-1} \equiv 1 \pmod{p} .$$

   Further, $1024 = 34 \cdot 30 + 4$, and hence,

   $$7^{1024} \equiv_{31} (7^{30})^{34} 7^4 \equiv_{31} 7^4 \equiv_{31} 7^2 7^2 \equiv_{31} (-13) \cdot (-13) \equiv_{31} 169 \equiv_{31} 14 .$$

   ANSWER: 14.

2. (3p) Draw three graphs G_1, G_2 and G_3, each with 12 vertices and 18 edges, with the following properties:

   (i) G_1 have an Euler circuit but no Hamiltonian cycle.

   (ii) G_2 have an Hamiltonian cycle but no Euler circuit

   (iii) G_3 have neither an Eulerian circuit nor an Hamiltonian cycle.

   Solution: We first draw four parallel edges between the vertices a and b. Then we mark the remaining 10 vertices on these four edges with at least two on each of these four edges, so there will be two vertices x and y that are not neighbors of a nor b. Every time you mark such a vertex you get a new edge, so in total we now

have 14 edges. Now draw edges from the vertices a and b to the vertices x and y. This will be the graph G_1, as every vertex has an even degree, and you must pass the vertex a more than once, if you will follow a route to all vertices.

Draw a cycle graph with 12 vertices a_1, a_2, ..., a_{12}. It does not matter how you fill in with further edges, this cycle will always constitute an Hamilton cycle of the graph. From the vertex a_1, draw edges to the vertices a_3, a_4, ..., a_8. The graph has now 18 edges and 12 vertices, but there are vertices of odd degree, for example the vertex a_3, so there will be no Euler circuit. This will be the graph G_2.

A disconnected graph can neither contain an Eulerian circuit nor an Hamilton cycle. Thus any disconnected graph can be the graph G_3.

3. (3p) In how many ways can the set $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ be partitioned into three subsets such that the elements 1, 2 and 3 will be placed in different sets?

   Solution: Place the elements in three different sets. For each of the remaining elements there are three possibilities, either to be placed in the set with the element 1, or the set with the element 2 or the set with the element 3. Hence,

   ANSWER: 3^7.

4. (3p) Let G denote the group $(Z_{24}, +)$. Find cosets S_1 and S_2 of two distinct non trivial subgroups H_1 and H_2, respectively, of G, with the property that S_1 and S_2 have exactly two elements in common of which one is the element 7.

   Solution: Let $H_1 = \{0, 12\}$ and $H_2 = \{0, 6, 12, 18\}$. Then, with

   $$S_1 = 7 + H_1 = \{7, 19\} \qquad S_2 = 7 + H_2 = \{1, 7, 13, 19\} ,$$

   the problem is solved.

5. (a) (1p) Let A denote a set of positive integers. Give a suitable definition of the concept greatest common divisor, below denoted $\gcd(A)$, of the numbers in the set A.

   Solution: The non negative integer D is the greatest common divisor to the integers in the set A if the following to conditions are satisfied

   (i) D divides all integers in the set A.

   (ii) if the integer d divides all integers in the set A then d divides D.

   (b) (2p) Show that for every non empty subset B of A it is true that $\gcd(A)$ divides $\gcd(B)$.

   Solution: We assume that $D = \text{sgd}(A)$ and $D' = \text{sgd}(B)$, respectively, always exist.

   From the condition (i) we get that D divides all integers in the set A and hence D will divide all integers in B, as B is a subset of A. By the condition (ii) this implies that $\text{sgd}(B)$ must be divisible by D, which was to be proved.

Part II

6. (3p) Find the number of integers n in the interval $1 \leq n \leq 1320$ such that n is not divisible by 10, 11 or 12.

   Solution: We will use the principle of inclusion exclusion and for that purpose we define the sets A, B and C that consists of those integers in the interval 1 to 320 that are divisible by 10, 11, and 12, respectively. Hence, the answer S is given by

   $$S = 1320 - |A \cup B \cup C| \, .$$

   We get that

   $$\begin{aligned} |A| &= \tfrac{1320}{10} &&= 132 \\ |B| &= \tfrac{1320}{11} &&= 120 \\ |C| &= \tfrac{1320}{12} &&= 110 \\ |A \cap B| &= \tfrac{1320}{\mathrm{mgm}(10,11)} &&= 12 \\ |A \cap C| &= \tfrac{1320}{\mathrm{mgm}(10,12)} &&= 22 \\ |B \cap C| &= \tfrac{1320}{\mathrm{mgm}(11,12)} &&= 10 \\ |A \cap B \cap C| &= \tfrac{1320}{\mathrm{mgm}(10,11,12)} &&= 2 \end{aligned}$$

   The formula for inclusion exclusion

   $$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$

   now gives the

   ANSWER: $1320 - 132 - 120 - 110 + 12 + 22 + 10 - 2 = 1000$.

7. (3p) Find an 1-error correcting linear code C with as many words as possible and such that

   (i) the word 10101011 belongs to C.

   (ii) the word 00111100 cannot be corrected.

   (iii) the word 11000011 can be corrected.

   Solution: We describe the code C by giving its parity check matrix $\mathbf{H}$. The number of columns is equal to eight, as the word length of the code is eight. These columns must be distinct, and distinct from the zero column, and hence, the number of rows must be at least equal to four (as else we can produce just seven distinct non zero columns if there were just three rows). Furthermore, the number of words of C, will be less the more linearly independent rows the matrix $\mathbf{H}$ has. By trial and error we find the following matrix with four rows and that satisfies the given conditions, and thus solves our problem:

   $$\begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}$$

8. (a) (2p) Find a non abelian (non commutative) group G with identity e with subgroups H_1, H_2, ..., H_k, where $k > 1$, of G such that $H_i \cap H_j = \{e\}$ for $i \neq j$, and such that

$$H_1 \cup H_2 \cup \ldots \cup H_k = G \, .$$

Solution: The group $\mathcal{S}_3$ consisting of all permutations of the set of elements $\{1, 2, 3\}$ has this property as it has the subgroups

$$H_1 =< (1\ 2) >, \quad H_2 =< (1\ 3) >, \quad H_3 =< (2\ 3) >, \quad H_4 =< (1\ 2\ 3) > ,$$

that just have the identity permutation in common and together cover the group $\mathcal{S}_3$.

(b) (2p) Assume that G is a group with the property that every element, except the identity, has the same order p, where p is a prime number. Show that G has subgroups H_1, H_2, ..., H_k, $k > 1$, that partition the set of non identity elements of the group G, in the same way as the subgroups in problem 8 (a) do.

Solution: We assume that the group G has a finite number of elements. Every element $a \neq e$ in G generates a subgroup $< a >$ of size p. The intersection of any two such subgroups, $< a > \cap < b >$, is a subgroup of both $< a >$ and $< b >$, and hence of an order that divides the prime number p. So, for any two elements $a, b \in G$, either

$$< a >=< b > ,$$

which means that $b \in < a >$, or

$$< a > \cap < b >= \{e\} ,$$

which is the case when $b \notin < a >$. Now recursively pick elements a_1, a_2, ..., a_n such that, for $k = 1, 2, \ldots, n$,

$$a_k \notin \cup_{i=1}^{k-1} < a_i > \ .$$

As the group G is finite, this procedure terminates after a finite number n of steps. Let $H_i =< a_i >$.

Alternatively, and in the infinite case, consider the set of subgroups

$$\{ < a > \mid \ a \in G \} ,$$

that has the property that any two distinct members of the set have the trivial intersection $\{e\}$ and the property that every element belongs to at least one member of the set.

(c) (1p) Let $p = 5$. Give an explicit example that demonstrates the facts in subproblem 8 (b).

Solution: Let $G = (Z_5, +) \times (Z_5, +)$. The following six subgroups of G will do:

$$\begin{aligned}
< (1,0) > &= \{(0,0),(1,0),(2,0),(3,0),(4,0)\},\\
< (0,1) > &= \{(0,0),(0,1),(0,2),(0,3),(0,4)\},\\
< (1,1) > &= \{(0,0),(1,1),(2,2),(3,3),(4,4)\},\\
< (2,1) > &= \{(0,0),(2,1),(4,2),(1,3),(3,4)\},\\
< (3,1) > &= \{(0,0),(3,1),(1,2),(4,3),(2,4)\},\\
< (4,1) > &= \{(0,0),(4,1),(3,2),(2,3),(1,4)\}.
\end{aligned}$$

Part III

9. Let $\mathcal{S}_n$ denote the set of all permutations of the elements in the set $\{1, 2, \ldots, n\}$. Two permutations α and β are said to commute if $\alpha\beta = \beta\alpha$. Below permutations are described by their cycle notation.

   (a) (1p) Find all elements in $\mathcal{S}_3$ that commute with the permutation $\alpha = (1\ 2\ 3)$.

   Solution: The set $\mathcal{S}_3$ have the six elements (1), (1 2), (1 3), (2 3), (1 2 3) and (1 3 2), and it is easy to check that
   ANSWER: only (1), (1 2 3) and (1 3 2) commute with (1 2 3).

   (b) (1p) Find five elements in $\mathcal{S}_5$ that commute with the permutation $\alpha = (1\ 2\ 3\ 4\ 5)$.

   Solution: As $\alpha \cdot \alpha^k = \alpha^{k+1} = \alpha^k \cdot \alpha$ we immediately get
   ANSWER: α, α^2, α^3, α^4 och $\alpha^5 = (1)$.

   (c) (3p) For every positive integer n, find all elements in $\mathcal{S}_n$ that commute with the permutation $\alpha = (1\ 2\ \ldots\ n)$.

   Solution: We first observe that as above we have that the n distinct permutations α^k, for $k = 1, 2, \ldots, n$, commute with α.
   If $\beta\alpha = \alpha\beta$ then $\beta\alpha\beta^{-1} = \alpha$. As $\alpha(i) = i + 1 \pmod{n}$, we get that

   $$\beta(i) = j \ \Rightarrow\ \beta(i+1) = \beta(\alpha(i)) = \beta(\alpha(\beta^{-1}(j))) = \beta\alpha\beta^{-1}(j) = \alpha(j) = j + 1\ .$$

   From the implication above follows recursively that the value of $\beta(i)$ is determined by the value of $\beta(1)$. There are at most n possible distinct values for $\beta(1)$ and thus there are not more than n distinct permutations that commute with α.
   We can thus conclude the following
   ANSWER: The permutations that commute with α are the permutations α^k, for $k = 1, 2, \ldots, n$.

10. We consider bipartite graphs with vertices in the sets X and Y with no edges between vertices in X and no edges between vertices in Y.

(a) (2p) Show that if $|X| \leq 10$, if the vertices in the sets X have a degree at least equal to 4, and if the vertices of Y have a degree less than or equal to 5, then there always exists a matching of size 8 in the bipartite graph.

Solution: See below

(b) (3p) Give and prove a theorem that generalizes the above situation, and from which the result in problem 10 (a) follows.

Solution: Let $\delta(v)$ denote the degree of the vertex v. Let $G(X \cup Y, E)$ denote a bipartite graph as described above, and with the set of edges E. Let, for every real number r, $\lfloor r \rfloor$ denote the largest integer k such that $k \leq r$.

Theorem 1 *In every bipartite graph $G(X \cup Y, E)$ such that for every $x \in X$ and $y \in Y$*

$$\delta(y) \leq M \leq m \leq \delta(x)$$

where m and M are integers, there exists a matching $\mathcal{M}$ of size

$$|\mathcal{M}| = \lfloor \frac{m}{M}|X| \rfloor \ .$$

Proof. Let $J(A)$ denote the joint in Y to the vertices in the subset A of X. Due to a theorem in the textbook it is sufficient to prove that for every subset A of X it is true that

$$|A| - |J(A)| \leq \Delta \ ,$$

where

$$\Delta = |X| - \lfloor \frac{m}{M}|X| \rfloor \ .$$

Let $N(A)$ denote the number of edges that are incident with a vertex in the subset A of X. Then, by counting the number of edges that are incident with a vertex in the subset $J(A)$ of Y we get that

$$m|A| \leq N(A) \leq M|J(A)| \ ,$$

and so

$$|J(A)| \geq \frac{m}{M}|A| \ ,$$

It follows that, for every subset A of X,

$$|A| - |J(A)| \leq |A| - \frac{m}{M}|A| = |A|(1 - \frac{m}{M}) \leq |X|(1 - \frac{m}{M}) \leq |X| - \lfloor \frac{m}{M}|X| \rfloor \ .$$

Example. Every bipartite graph $G(X \cup Y, E)$ such that $|X| = 10$, $m = 4$ and $M = 5$ admits a matching $\mathcal{M}$ of size

$$|\mathcal{M}| = \lfloor \frac{4}{5}10 \rfloor = 8 \ .$$

Note You can get 5p on problem 10 by first solving the (b)-problem and then showing how the result in (a) follows from the solution of problem (b).