Matematiska Institutionen
KTH

Exam to the course Discrete Mathematics, SF2736, April 9, 2015, 08.00-13.00.

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. (a) (1p) Find $535^{176}(\text{mod } 89)$.

   Solution. As 89 is a prime number, and 89 does not divide 535, we can use a theorem of Fermat and get

$$535^{176} \equiv_{89} (535^{88})^2 \equiv_{89} 1^2 \equiv_{89} 1.$$

   (Or why not use the fact that $535 \equiv 1(\text{mod } 89)$.)
   Thus
   ANSWER: 1.

   (b) (2p) Solve in the ring Z_{53} the matrix equation

$$\begin{pmatrix} 10 & 12 \\ 13 & 14 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

Solution.

$$\left\{ \begin{array}{rcrcr} 10x & + & 12y & = & 1 \\ 13x & + & 14y & = & 0 \end{array} \right. \sim \left\{ \begin{array}{rcrcr} 10x & + & 12y & = & 1 \\ 3x & + & 2y & = & -1 \end{array} \right. \sim$$

$$\left\{ \begin{array}{rcrcr} -8x & + & & = & 7 \\ 3x & + & 2y & = & -1 \end{array} \right.$$

We need to find the inverse of 8 in the ring Z_{53}:

$$53 = 7 \cdot 8 - 3, \qquad 8 = 3 \cdot 3 - 1$$

which gives that

$$1 = 3 \cdot 3 - 8 = 3(7 \cdot 8 - 53) - 8 = 20 \cdot 8 - 3 \cdot 53.$$

Thus

$$x = -20 \cdot 7 = 19.$$

We then get

$$2y = -1 - 3 \cdot 19 = -5$$

ANSWER: $x = 19$ and $y = 48$.

2. (3p) In how many ways can 10 boys and 13 girls be placed in a row in such a way that no two boys are adjacent.

   Solution. We first place the girls in a row, which can be done in 13! distinct ways. Then we choose where to place the boys, there are 14 distinct positions between, in front or at the rear of the row of girls for the 10 boys, and placing the boys can then be performed in 10! distinct ways. Thus in total
$$13!\binom{14}{10}10!.$$

   ANSWER: 13!14!/4!.

3. Let G denote the group which is the direct product $G = (Z_4, +) \times (Z_6, +)$.
   (a) (1p) Find and describe a cyclic subgroup H to G of size $|H| = 12$.

   Solution. The group $(Z_6, +)$ has a subgroup of size 3, the set of elements $K = \{0, 2, 4\}$. The set $(Z_4, +) \times K$ constitute a subgroup of size 12.

   (b) (1p) Is there any cyclic subgroup K to G of size $|K| = 8$.

   Solution. No.

   (c) (1p) Find the number of subgroups to G of size 2.

   Solution. A subgroup of size 2 is cyclic and generated by an element of order 2. We enumerate the elements of order 2:
$$(2, 0), \quad (0, 3), \quad (2, 3).$$
   Thus
   ANSWER: 3.

4. (3p) Solve, by using the technique with generating functions, the recursion
$$a_n = a_{n-1} + 12a_{n-2}, \qquad n = 2, 3, \ldots$$
   where $a_0 = 2$ and $a_1 = 1$

   Solution. Let
$$A(t)\sum_{n=0}^{\infty} a_n t^t.$$
   We multiply the recursion with t^n, and sum for $n = 2, 3, \ldots$:
$$\sum_{n=2}^{\infty} a_n t^n = \sum_{n=2}^{\infty} a_{n-1} t^n + 12\sum_{n=2}^{\infty} a_{n-2} t^n$$
   and thus
$$A(t) - a_1 t - a_0 = t(A(t) - a_0) + 12t^2 A(t).$$
   Hence
$$(1 - t - 12t^2)A(t) = t + 2 - 2t$$
   We get
$$A(t) = \frac{t-1}{1-t-12t^2} = \frac{2-t}{(1-4t)(1+3t)} = \frac{C}{1-4t} + \frac{D}{1+3t}.$$

Simple calculations gives $C = 1$ and $D = 1$. Consequently,

$$A(t) = \frac{1}{1-4t} + \frac{1}{1+3t} = \sum_{n=0}^{\infty}(4t)^n + \sum_{n=0}^{\infty}(-3t)^n = \sum_{n=0}^{\infty}(4^n + (-3)^n)t^n.$$

ANSWER: $a_n = 4^n + (-3)^n$

5. (a) (1p) Is there any connected graph G, without multiple edges and loops, with 11 vertices of the degrees (valencies) 1, 2, 3, 4, ..., 11, respectively.

   Solution. No, as the number of vertices is 11, the number of neighbors of a vertex is at most 10. Thus no vertex can have degree 10.

   (b) (2p) Find the minimum number of edges that must be deleted in the complete graph K_n so that the graph that remains will not be connected.

   Solution. When the minimum number of edges is deleted, two components will remain, that both are complete graphs, the graphs K_x and K_y, where $x + y = n$. The number edges deleted is then the maximum number of edges in a bipartite graph vertex sets X and Y with x and $y = n - x$ vertices, respectively, that is the number of edges in the complete bipartite graph $K_{x,n-x}$, which is

   $$f(x) = x(n-x), \qquad 1 \leq x \leq n-1.$$

   The minimum value $n - 1$ of this function occurs when $x = 1$, and $x = n - 1$.
   ANSWER: $n - 1$.

Part II

6. (a) (1p) Give a formula for the number of words with n letters of which m are identical and the remaining letters distinct.

   Solution. First choose the places for the m identical letters, which can be done in

   $$\binom{n}{m} = \frac{n!}{m!(n-m)!}$$

   ways. Then order the remaining $n - m$ letters for the remaining places, which can be done in

   $$(n-m)!$$

   ways. Thus we get
   ANSWER:

   $$\frac{n!}{m!}$$

   (b) (2p) Prove the identity.

   $$\sum_{i=0}^{k} \binom{n+i}{i} = \binom{n+k+1}{k}.$$

Solution. Proof by induktion. It is true that

$$\sum_{i=0}^{1} \binom{n+i}{i} = \binom{n}{0} + \binom{n+1}{1} = 1 + (n+1) = \binom{n+2}{1}.$$

The induction step is as follows

$$\sum_{i=0}^{k} \binom{n+i}{i} + \binom{n+(k+1)}{k+1} = \binom{n+k+1}{k} + \binom{n+(k+1)}{k+1} =$$

$$= \binom{n+(k+1)+1}{k+1}.$$

This completes the proof for the cases $k = 1, 2, \ldots$. The case $k = 0$ is trivial.

7. (4p) Find the minimum and maximum number of edges in a bipartite graph with 53 vertices admitting an Euler circuit.

Solution. We first consider the maximum number. Consider the complete bipartite graph $K_{n,53-n}$, where, with standard notation, $|X| = n$ and $|Y| = 53 - n$. Without loss of generality we may assume that n is an odd number. The graph is connected and the number of edges is $n(53 - n)$. As the vertices in the Y-set has the odd degree n, we cannot obtain an Euler circuit unless we delete at least one edge from each Y-vertex, that is deleting at least $53 - n$ edges. It remains

$$f(n) = (n-1)(53-n)$$

edges. As, with $m = n - 1$

$$f(n) = g(m) = m(52 - m),$$

its maximum value appears when $m = 26$, that is $n = 27$.

We now show that such a bipartit graph exists. Again consider $K_{27,26}$ with

$$X = \{x_1, \ldots, x_{27}\}, \qquad Y = \{y_1, \ldots, y_{26}\}.$$

If we delete the edges

$$x_k y_{2k-1}, \quad x_k y_{2k}, \qquad k = 1, 2, \ldots, 13,$$

then all vertices have an even degree, and the graph is connected, as all Y-vertices are neighbors of x_{27}, and every X-vertice is a neighbor to at least one Y-vertex.

Now to the minimum number. All cycles in a bipartite graph has an even length, thus an Euler circuit in a bipartite graph on 53 vertices must have at least 54 edges. We now define such a bipartite graph. Simply take a cycle with 50 vertices

$$v_1 v_2 \ldots v_{50} v_1$$

and a cycle

$$v_{50} v_{51} v_{52} v_{53} v_{50},$$

together these cycles constitute an Euler circuit. This graph has 54 edges, all cycles have an even length, and thus the graph is bipartite.

8. (4p) Let G denote group of (multiplicatively) invertible elements in the ring Z_{32}. For which integers n is there a group of permutations $\mathcal{S}_n$ of the elements in the set $\{1, 2, \ldots, n\}$ such that $\mathcal{S}_n$ contains a subgroup isomorphic with G.

   Solution. The invertible elements in Z_{32} are

   $$G = \{1, 3, 5, 7, \ldots, 31\}$$

   so the size of G is $|G| = 16$. We investigate this group, according to the order of its elements. The order of 3 divides 16, so we check 3^d where d divides 16:

   $$3^2 = 9 \neq 1, \qquad 3^4 = 17, \qquad 3^8 = 1.$$

   Hence 3 generates a subgroup H of size 8:

   $$H = \langle 3 \rangle = \{3, 9, 27, 17, 19, 25, 11, 1\}$$

   The element -1 has order 2, and generates a subgroup K:

   $$K = \langle -1 \rangle = \{-1, 1\}.$$

   As easily seen every element $g \in G$ can be written

   $$g = hk = kh$$

   for unique elements $h \in H$ and $k \in K$, as

   $$G = \langle 3 \rangle = \{\pm 3, \pm 9, \pm 27, \pm 17, \pm 19, \pm 25, \pm 11, \pm 1\}.$$

   We can conclude that $\mathcal{S}_n$ must contain two disjoint cyclic subgroups of order 8 and 2, respectively. For $n \geq 10$ this is true, and indeed, the subgroup of $\mathcal{S}_n$ generated by the permutations

   $$\gamma = (1\ \ 2\ \ 3\ \ 4\ \ 5\ \ 6\ \ 7\ \ 8), \qquad \psi = (9\ \ 10)$$

   is isomorphic to G, by the isomorphism

   $$\varphi(3^d(-1)^e) = \gamma^d \psi^e.$$

   ANSWER: For $n \geq 10$.

Part III

9. Let D be the smallest linear code containing the words 11111111, 10011001 and 11100001.

   (a) (1p) Show that D is a 1-error-correcting code.

   Solution. The code contains all possible linear combinations of the three given words, which is the set

   $$D = \{11111111, 10011001, 11100001, 01100110, 00011110,$$

   $$01111000, 11100001, 10000111\}$$

   As the code is linear, its minimum distance is equal to the minimum non-zero weight, which is 4. As minimum distance is greater than 3, the code is 1-error-correcting.

(b) (2p) Find two distinct 1-error-correcting codes C_1 and C_2 distinct from D and containing D. (1p for each such code.)

Solution. We add another generator to the given set of four generators, so

$$C_1 = \text{span}\{11111111, 10011001, 11100001, 01010101\},$$

and

$$C_2 = \text{span}\{11111111, 10011001, 11100001, 01010011\},$$

are 1-error-correcting codes. Indeed their parity-check matrices are

$$\mathbf{H}_1 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{bmatrix}, \quad \mathbf{H}_2 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \end{bmatrix},$$

respectively. As the columns are distinct, the codes are 1-error-correcting, the words $01010101 \in C_1$ and $01010011 \in C_2$ are at distance 2 and can thus not belong tothe same 1-error-correcting code. Hence, $C_1 \neq C_2$.

(c) (3p) Give a non-trivial upper bound for the number of linear 1-error-correcting codes C that contain D.

Solution. As the length of a 1-error-correcting code C containing D is 8, the packing condition gives that

$$|C| \leq \frac{2^8}{1 + \binom{8}{1}} < 29,$$

and as the number of words in a linear 1-error-correcting code is a power of two (and as $|D| = 8$), we may conclude that $|C| = 16$. Furthermore we note that

$$C = D \cup \{\bar{c} + D\},$$

for some code word $\bar{c} \in C$ (compare the solution of previous subproblem). The number of cosets to D in Z_2^8 is, including D, equal to $2^8/|D| = 32$. A trivial bound for the number of 1-error-correcting codes containing C would be 32. To get a non-trivial bound we exclude cosets $\bar{c} + D$ containing words at distance less than 3 to words of D. A non-trivial bound is thus given by excluding the cosets

$$\bar{e}_i + C,$$

where $\bar{e}_i$ is a word of weight 1 with its single non-zero element in position i. As minimum distance in D is four, no two such words belong to the same coset. Thus at least 8 cosets will not produce, together with D, a 1-error-correcting code. Thus a non-trivial upper bound would, for the number of 1-error-correcting codes C containing D, be $32 - 8$, that is 24. (Indeed, the true value is far from this value, but not a necessity to achieve for getting three marks on this subproblem).

10. (4p) Is the set of all equivalence relations on the set of positive integers an uncountable or a countable infinite set? Justify your answer with good motivations.

Solution. The set of all equivalence relations on the set of positive integers is uncountable infinite. To verify this we consider the subset $\mathcal{E}$ of all such equivalence relations that partitions the set of positive integers into two equivalence classes, C_1 and C_2. As the number family of subsets of the set of positive integers is uncountable infinite the result follows. Indeed, there is an uncountable infinite set possibilities for C_1 and C_2, respectively. However, concerned with equivalence classes, they are not labeled, thus, every equivalence relation will be counted twice. Nevertheless, the half of an infinite uncountable set is itself uncountable and infinite.