Matematiska Institutionen
KTH

Solutions to the exam to the course Discrete Mathematics, SF2736, May 31, 2013, 08.00–13.00.

Examiner: Olof Heden.

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. (a) (1.5p) Find $\gcd(789, 1011)$.

Solution. The algorithm of Euclides gives

$$\begin{array}{rcrcrcr} 1011 & = & & & 789 & + & 222 \\ 789 & = & 4 & \cdot & 222 & - & 99 \\ 222 & = & 2 & \cdot & 99 & + & 24 \\ 99 & = & 3 & \cdot & 24 & + & 3 \\ 24 & = & 8 & \cdot & 3 & & \end{array}$$

ANSWER: 3

(b) (1.5p) Find $34^{50} (\bmod 78)$.

Solution. We use the theorem of Euler. As $78 = 2 \cdot 3 \cdot 13$, we get

$$\varphi(78) = 78(1 - \frac{1}{2})(1 - \frac{1}{3})(1 - \frac{1}{13}) = 24.$$

Hence

$$34^{50} \equiv_{78} (34^{24})^2 \cdot 34^2 \equiv_{78} 1^2 \cdot 17 \cdot 68 \equiv_{78} 17(-10) \equiv_{78} -170 \equiv_{78} -14.$$

ANSWER: 64.

2. (3p) A connected graph G has 13 vertices, no multiple edges or loops. Which are the possibilities for the number of edges of G.

   Solution. A tree on 13 vertices has 12 edges. If any edge of a tree is deleted the remaining graph will be disconnected. The minimum number of edges is thus 12. The complete graph K_{13} on the vertices in the set $V = \{1, 2, \ldots, 13\}$ has 78 edges as every edge corresponds to a 2-subset $\{x, y\}$ of V, and the number of 2-subsets to a set with 13 elements is $13 \cdot 12/2$.

   Consider the subgraph T of K_{13} having the edges

   $$E = \{\{1, 2\}, \{2, 3\}, ..., \{12, 13\}\}$$

   Taking away any set of n edges from the edgeset of K_{13}, except any from the set E will give a connect graph with $78 - n$ edges. Thus

   ANSWER: The number of edges can be any integer e in the interval $12 \leq e \leq 78$.

3. (3p) Let G be a cyclic group with 48 elements generated by the element g. There is one and only one subgroup H to G of size 12. Show that H is cyclic and find all generators of H.

   Solution. Assume that the element g of G generates G. The subgroup H to G generated by $h = g^4$ has twelve elements

   $$H = \langle h \rangle = \{h = g^4, h^2 = g^8, \ldots, h^{12} = g^{48} = e\}.$$

   An element k in H generates a subgroup of H with as many elements as the order of k. We get that the group

   $$H_6 = \langle h^2 \rangle = \{h^2, h^4, h^6, h^8, h^{10}, h^{12} = e\}$$

   is a subgroup of H with six elements all of an order that divides six. Similarly we get

   $$H_4 = \langle h^3 \rangle = \{h^3, h^6, h^9, e\}, \quad H_3 = \{h^4, h^8, e\}, \quad H_2 = \{h^6, e\}.$$

   The elements not contained in any of these four subgroups to H have order twelve. We thus get

   ANSWER: The elements $h = g^4$, $h^5 = g^{20}$, $h^7 = g^{28}$, and $h^{11} = g^{44}$.

4. (3p) Find the generating function to the sequence a_0, a_1, ..., where $a_0 = 2$, $a_1 = 3$ and $a_n = a_{n-1} - 6a_{n-2}$, for $n = 2, 3, \ldots$.

   Solution. For $n = 2, 3, \ldots$ we get the equalities

   $$a_n t^n = t a_{n-1} t^{n-1} - 6t^2 a_{n-2} t^{n-2}.$$

   The requested generating function is $A(t) = \sum_{n=0}^{\infty} a_n t^n$. By using the set of equalities above we can derive the following equation for $A(t)$:

   $$A(t) - a_1 t - a_0 = t(A(t) - a_0) - 6t^2 A(t).$$

Simplifications then give

$$A(t) = \frac{2+5t}{1-t+6t^2}.$$

Hence

ANSWER: $(2+5t)/(1-t+6t^2)$

5. (3p) Nine distinct guys shall ride in a row on bicycles. How many distinct rows can then be formed if there are four green bikes, three red bikes and two yellow bikes, else the bikes are indistinguishable.

   Solution. We first place the bikes in a row. The number of ways this can be done is given by a multinomial coefficient

   $$\binom{9}{4,3,2} = \frac{9!}{4! \cdot 3! \cdot 2!}.$$

   Then we place the guys on the nine bikes, which can be done in 9! distinct ways. Consequently

   ANSWER: $9! \cdot 9!/4! \cdot 3! \cdot 2!$.

Part II

6. (3p) Let p be a prime number. Show that if $p > 3$ then 24 divides $p^2 - 1$.

   Solution. We note that

   $$p^2 - 1 = (p-1)(p+1).$$

   Of three consecutive integers exactly one is divisible by three. As 3 does not divide p, the integer 3 must divide either of $p-1$ or $p+1$. Hence, 3 divides p^2-1. The prime number p is odd, hence both $p-1$ and $p+1$ are even, of which one is divisible by 4. Hence, $2 \cdot 4$ divides $(p-1)(p+1)$. As both 3 and 8 divides p^2-1 we are done.

7. (4p) Let $\mathcal{S}_8$ denote the set of all permutations of the set $\{1, 2, \ldots, 8\}$. Write the permutation $\varphi = (1\ \ 3\ \ 5)(2\ \ 4\ \ 6\ \ 7)$ as a product of nine distinct permutations in $\mathcal{S}_8$ of which no two are inverses to each other, that is,

   $$\varphi = \psi_1 \psi_2 \cdots \psi_9, \qquad \text{and} \qquad \psi_i \psi_j \neq \text{Id}.$$

   for $i \neq j$, or show that this is impossible, (if this happens to be the case).

   Solution. There are indeed very many distinct possibilities. Here is one:

   $$\varphi = (1\ \ 5)(1\ \ 3)(2\ \ 7)(2\ \ 6)(2\ \ 4)(1)\psi\psi^2\psi^3$$

   where

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

8. (4p) In how many ways can the set $\{1, 2, \ldots, 8\}$ be divided into three mutually disjoint subsets each containing at least two elements.

   Solution. There are two cases to treat, either there are two sets each with two elements and one set with four elements, or one set with two elements and two subsets with three elements each.

   In treating the first case we start by choosing four elements to the 4-set. This can be done in $\binom{8}{4}$ distinct ways. Remains four elements $\{a_1, a_2, a_3, a_4\}$ to divide into two sets of size two. The element a_1 must then have exactly one set mate among the remaining three. There are three possibilities for this. So in total this case the total number of possibilities is

$$3 \cdot \binom{8}{4} = 3\,\frac{8 \cdot 7 \cdot 6 \cdot 5}{1 \cdot 2 \cdot 3 \cdot 4} = 210.$$

   Similarly, in the second case, we get that the number of possible values is

$$\binom{8}{2}\binom{5}{2} = \frac{8 \cdot 7}{1 \cdot 2}\frac{5 \cdot 4}{1 \cdot 2} = 28 \cdot 10 = 280.$$

   ANSWER: 490.

Part III

9. A set C of binary words of length n is a covering 1-code in Z_2^n if every binary word of length n is within distance at most one from at least one word of C.

   (a) (1p) Show that the words in the set

$$C = \{0000, 1100, 1010, 1001, 0110, 0101, 0011, 1111\}$$

   is a covering 1-code in Z_2^4.

   Solution The code C consists of all words of even weight. If you add a word of weight one to any word of odd weight, you will get a word of even weight. Hence all words of odd weight are at distance one from at least one code word. The even weight words are already code words.

   (b) (1p) Are there any covering 1-codes in Z_2^4 with fewer words? An answer must contain a motivation.

   Solution. Let C be the null space, when counting modulo 2, of the matrix

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

   As being a null space of a matrix we get that C is a subspace of Z_2^4 of dimension 2 and thus contains exactly $2^2 = 4$ elements. Assume $\bar{x} = (x_1 \ \ldots \ x_4)$ not in

C. Then, $\mathbf{H}\bar{x}^T$ will be equal to one of the columns in $\mathbf{H}$. Hence, $\bar{x}$, can be "corrected" to at least one word of C, by using the general error-correcting procedure using parity-check matrices.

Thus

ANSWER: Yes.

(c) (3p) A code C is linear if the difference between any two words of C also belongs to C. Find a construction of linear covering 1-codes, and discuss whether your construction is "the best possible".

Solution. Every subspace of a vector space is a null space of a matrix. Thus the requested linear code is the null space in the vector space Z_2^n of a matrix $\mathbf{H}$ with n columns and k linearly independent rows.

Let $\bar{e}_i$ denote the word of weight one with its only non-zero entry in position i. If C is a covering code, then for every $\bar{x}$ in $Z_2^n \setminus C$ it must be true that

$$\mathbf{H}(\bar{x}^T + \bar{e}_i^T) = \bar{0}^T,$$

or equivalently

$$\mathbf{H}\bar{x}^T = \mathbf{H}\bar{e}_i^T,$$

for at least one coordinate position i.

We know that $\mathbf{H}\bar{e}_i^T$ is equal to column number i of $\mathbf{H}$. As this matrix has full rank, to every column of height k there is a vector $\bar{x}$ such that $\mathbf{H}\bar{x}^T$ is equal to that column. Hence, if C is a covering code if and only if every possible non-zero column of height appears at least once in $\mathbf{H}$.

The construction is thus as follows. For given length n, choose the largest k such that $2^k - 1 \leq n$. Form a matrix $\mathbf{H}$ with n columns and k rows and with all non-zero columns appearing in the this matrix. The null space of $\mathbf{H}$ will be the best possible linear covering code of length n.

10. (5p) (From Wilson: Introduction to Graph Theory.) Let G be a bipartite graph with vertex sets X and Y, so that there are no edges between vertices in X, and no edges between vertices of Y. Suppose that every vertex in X has a valency at least equal to the integer t and suppose that the Hall condition is satisfied. Show that the number of complete matchings in G is at least equal to $t!$ if $|X| \geq t$, and is at least equal to $t!/(t - |X|)!$ if $|X| < t$.

Solution. If the Hall condition $|A| \leq |J(A)|$, for every subset A of X, then this condition is satisfied whenever deleting one vertex form X. So we can proceed by induction on the number of vertices of X.

Let t be fixed.

We first consider the case $|X| < t$. Denote the vertices in X by $v_1, \ldots, v_n$. Match v_n with any of t adjacent vertices. By induction hypothesis, the remaining bipartit graph admits at least $(t-1)!/(t-1-(|X|-1))!$ distinct complete matchings. Hence by principle of multiplication we get $t!/(t - |X|)!$ distinct complete matchings. The initial step $|X| = 1$ is a complete triviality.

In the case $t = |X|$ we achieve at least $t!$ distinct complete matchings with exactly the same arguments as above.

The case $t < |X|$ can now be treated by induction over the size of X.