Matematiska Institutionen
KTH

Exam to the course Discrete Mathematics, SF2736, March 13, 2014, 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.

Part I

1. (3p) Find all solutions in the ring Z_{56} to the system of equations

$$\begin{cases} 4x + 7y = 5 \\ 3x + 2y = 8 \end{cases}$$

Solution. Gauss eliminations give the following systems with the same solution set as the system above

$$\begin{cases} x + 5y = -3 \\ 3x + 2y = 8 \end{cases} \iff \begin{cases} x + 5y = -3 \\ 0x - 13y = 17 \end{cases}$$

The inverse of 13 in the ring Z_{56} is found by using the algorithm of Euclid:

$$56 = 4\cdot 13+4, \quad 13 = 3\cdot 4+1, \quad \Rightarrow \quad 1 = 13-3\cdot 4 = 13-3(56-4\cdot 13) = 13\cdot 13-3\cdot 56$$

Thus, $13 \cdot 13 = 1$ in the ring Z_{56}, so

$$y = -13 \cdot 17 = -221 = -4 \cdot 56 + 3,$$

and consequently

$$x = -3 - 5y = -3 - 5 \cdot 3 = -18 = 38.$$

ANSWER: $(x, y) = (38, 3)$.

2. (3p) Solve, by using the technique with generating functions, the recursion

$$a_n = 3a_{n-1} + 2^n, \qquad n = 1, 2, \ldots, \qquad a_0 = 1.$$

Solution. Let $A(t) = \sum_{n=0}^{\infty} a_n t^n$. From the sequence of equalities below

$$a_n t^n = 3t a_{n-1} t^{n-1} + 2^n t^n, \qquad n = 1, 2, 3, \ldots$$

we deduce that

$$\sum_{n=0}^{\infty} a_n t^n - a_0 = 3t \sum_{n=0}^{\infty} a_n t^n + \sum_{n=1}^{\infty} (2t)^n$$

Hence, as $a_0 = 1$

$$(1-3t)A(t) = 1 + \frac{2t}{1-2t} = \frac{1}{1-2t}$$

or equivalently, expanding in partial fractions

$$A(t) = \frac{1}{(1-2t)(1-3t)} = \frac{3}{1-3t} - \frac{2}{1-2t}.$$

Hence,

$$A(t) = 3\sum_{n=0}^{\infty} (3t)^n - 2\sum_{n=0}^{\infty} (2t)^n = \sum_{n=0}^{\infty} (3^{n+1} - 2^{n+1}) t^n.$$

ANSWER: $3^{n+1} - 2^{n+1}$.

3. (3p) Find the number of ways to distribute 18 identical marbles in the boxes no. 1, no. 2, ..., no. 6, such that the total number of marbles distributed in box no. 1 to no. 4 is twice as many as the number of marbles distributed in the boxes no. 5 and no. 6.

Solution. Trivially, twelve of the marbles are distributed in the first four boxes and the remaining six in the remaining two. As the number of ways to distribute n identical objects in k distinct boxes is equal to

$$\binom{n+k-1}{k-1}$$

we get

ANSWER:

$$\binom{15}{3}\binom{7}{1} = \frac{15 \cdot 14 \cdot 13}{1 \cdot 2 \cdot 3} \cdot 7 = 3185.$$

4. (3p) Find the number of cyclic subgroups to the group $(Z_2, +) \times (Z_3, +) \times (Z_4, +)$.

Solution. The group $(Z_3, +) \times (Z_4, +)$ is a cyclic group of order 12, which thus is isomorphic to the group $(Z_{12}, +)$, (as cyclic groups of the same order are isomorphic).

We thus count the number of cyclic subgroups of the group $G = (Z_2, +) \times (Z_{12}, +)$.

In order to simplify our enumeration of all cyclic subgroups, we will use the fact that if the cyclic group $H = \langle g \rangle$ generated by g has size, or order, n, then

$$\langle g \rangle = \langle g^k \rangle \qquad \Longleftrightarrow \qquad \gcd(n, k) = 1.$$

Furthermore, g is a generator of the cyclic subgroup H of G if and only if the element g has order $|H|$.

We thus get the following cyclic subgroups of G:

$$H_{t,1} = \langle (t,1) \rangle = \langle (t,5) \rangle = \langle (t,7) \rangle = \langle (t,11) \rangle, \qquad H_{t,2} = \langle (t,3) \rangle = \langle (t,9) \rangle,$$

$$H_{t,3} = \langle (t,2) \rangle = \langle (t,10) \rangle, \quad H_{t,4} = \langle (t,4) \rangle = \langle (t,8) \rangle, \quad H_{t,5} \langle (t,6) \rangle \quad H_{t,6} = \langle (t,0) \rangle,$$

where $t \in (Z_2, +)$. Hence,

ANSWER: There are in total 12 cyclic subgroups.

5. (3p) Show that a graph with $2n-3$ vertices cannot be connected if n of the vertices have valency 1 and the remaining vertices have either valency 2 or 3.

   Solution. If the graph with $2n-3$ vertices is connected then it has a spanning tree with $2n-4$ edges. We estimate the number of edges $|E|$

$$2|E| = \sum_{v \in V} \delta(v) \leq n \cdot 1 + (n-3) \cdot 3 = 4n - 9 < 2(2n-4).$$

   This proves the statement.

Part II

6. (3p) How many arrangements are there of $a, a, a, b, b, b, c, c, c, d, d, d$ without three consecutive letters the same.

   Solution. We use the principle of inclusion-exclusion. Let X denote the set of words with the three consecutive letters xxx, for $x = a, b, c, d$. By considering xxx as one letter we deduce the following

$$|A| = |B| = |C| = |D| = \binom{10}{1,3,3,3}.$$

   For $X \neq Y$, we get

$$|X \cap Y| = \binom{8}{1,1,3,3},$$

   and similarly for the remaining cases to consider. Thus

   ANSWER:

$$\binom{12}{3,3,3,3} - \binom{4}{1}\binom{10}{1,3,3,3} + \binom{4}{2}\binom{8}{1,1,3,3} - \binom{4}{3}\binom{6}{1,1,1,3} + \binom{4}{1,1,1,1}.$$

7. Let $\mathcal{S}_5$ denote the group of all permutations of the elements in the set $\{1,2,3,4,5\}$ and let $\mathcal{M}$ denote the following subset of $\mathcal{S}_5$:

$$\mathcal{M} = \{(1\ \ 2\ \ 3), (2\ \ 4), (2\ \ 5), (3\ \ 5)\}.$$

(a) (2p) Find the least, according to size, subgroup H of $\mathcal{S}_5$ that contains the set $\mathcal{M}$.

Solution. We first note the following:

$$(x\ \ y)(x\ \ z)(x\ \ y) = (y\ \ z). \tag{1}$$

Hence we may deduce that

$$(2\ \ 4)(2\ \ 5)(2\ \ 4) = (4\ \ 5) \in H.$$

We also note that H contains the element

$$(1\ \ 2\ \ 3)(3\ \ 5)(1\ \ 3\ \ 2) = (1\ \ 5)$$

Thus, we may deduce from relation (1), as $(5\ \ x) \in H$, for $x = 1, 2, 3, 4$, that

$$\{(x\ \ y) \mid x, y \in \{1, 2, 3, 4, 5\}\} \subseteq H.$$

As every permutation can be written as a product of 2-cycles we get that H is the full group $\mathcal{S}_5$.
ANSWER: $H = \mathcal{S}_5$

(b) (1p) Is there a subset of $\mathcal{M}$ that gives the same result as in the problem above.

Solution. Yes, we can delete the permutation $(3\ \ 5)$ from the set $\mathcal{M}$. As above we can deduce that

$$(1\ \ 2\ \ 3)(2\ \ 5)(1\ \ 3\ \ 2) = (3\ \ 5) \in H.$$

Then we can continue as above.

8. (5p) Find all positive integers n less than 1 000 such that $12^{41} \equiv 1 (\text{mod } n)$ and $7^5 \equiv 1 (\text{mod } n)$.

Solution. We first observe that $\gcd(n, 12) = 1$ and $\gcd(7, n) = 1$, as the elements 7 and 12 in the ring Z_n are invertible. So for $n < 12$ the only possible candidates are $n = 5$ and $n = 11$. We note that

$$7^5 \equiv_5 2^5 \equiv_5 2 \neq 1, \qquad 7^5 \equiv_{11} (-4)^2(-4)^2(-4) \equiv_{11} 5 \cdot 5 \cdot (-4) \equiv_{11} -12 \equiv_{11} -1 \neq 1.$$

Thus, neither $n = 5$ nor $n = 11$ satisfies all given conditions on n.

We now consider the rings Z_n where $n \geq 13$, and consider 7 and 12 as elements of these rings. The elements 7 and 12 are invertible in these rings. The set of invertible elements in Z_n constitute a group $U(Z_n)$. The size of $U(Z_n)$ is $\varphi(n)$, the number of elements of Z_n relatively prime to n. It is well known that

$$n = p_1^{e_1} \cdots p_k^{e_k} \qquad \Longrightarrow \qquad \varphi(n) = p_1^{e_1 - 1} \cdots p_k^{e_k - 1}(p_1 - 1) \cdots (p_k - 1), \tag{2}$$

where p_1, p_2, ..., p_k are distinct prime numbers. We also know that the order of an element in a group divides the size of the group. As 12 has the order 41 and

7 has order 5 in $U(Z_n)$ we can conclude that both 41 and 5 divides $\varphi(n)$. From Equation (2) we thus deduce that either $p_i = 41$ and $e_i \geq 2$ for some i and/or 41 divides $p_i - 1$, and similarly for the prime number 5.

We note that $41^2 > 1\,000$ and $25 \cdot 42 > 1\,000$. Hence, as we assume that $n \leq 1\,000$ we can conclude that the only possibility is that 41 divides $p_i - 1$ for some i, and 5 divides $p_j - 1$ for some j not necessarily distinct from i.

If $i \neq j$ we get that $p_i \geq 83$ and $p_j \geq 11$, which gives the only possible value of $n < 1000$ to be $n = 11 \cdot 83 = 913$. If $i = j$ then we look for a prime number p_i such that $41 \cdot 5$ divides $p_i - 1$. Candidates are thus $n = k \cdot 205 + 1$ which gives the integers 206, 411, 616, and 821 to check whether or not they are prime numbers. As 3 divides 411, and 2 divides both 206 and 616, it remains to check $n = 821$. (A trivial check of divisibility for primes less than 29 gives that none of the primes 3, 5, 7, 11, 13, 17, 19 and 23 divides 821 confirming that 821 is a prime number. This is not a necessary check, see below.)

Summarizing, it remains just two candidates for n, $n = 821$ and $n = 913$.

Now $7^5 - 1 = 16806$ which is not divisible 913, as it is not divisible by 11. Furthermore

$$16806 = 20 \cdot 821 + 386.$$

Thus 7^5 is not congruent to 1 modulo n for neither $n = 821$ nor $n = 913$.

ANSWER: No integer in the interval $1 \leq n \leq 1000$ satisfies the given condition.

Part III

9. (a) (1p) Explain why the two parity-check matrices $\mathbf{H}$ and $\mathbf{H}'$ below define the same 1-error-correcting code:

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

Solution. Denote by C, the 1-error-correcting code with the parity-check matrix $\mathbf{H}$. The row space of the two matrices above are the same, as the matrix $\mathbf{H}'$ is obtained from $\mathbf{H}$ by adding the first row of $\mathbf{H}$ to the second row. As the code C is defined to be the null space of the matrix $\mathbf{H}$, elementary linear algebra arguments give that C also is the null space of the matrix $\mathbf{H}'$.

(b) (2p) Assume that the 1-error-correcting code C of length $n = 2^k - 1$ is defined by its parity-check matrix $\mathbf{H}$ of size $k \times n$. Every permutation φ of the set of coordinate positions induces a permutation of the set of words of C, by

$$\varphi : \ \bar{c} = (c_1, c_2, \ldots, c_n) \quad \mapsto \quad \varphi(\bar{c}) = (c_{\varphi^{-1}(1)}, c_{\varphi^{-1}(2)}, \ldots, c_{\varphi^{-1}(n)}).$$

Explain why if $\varphi(C) = C$ then there is a $k \times k$-matrix $\mathbf{A}$ such that column number i of $\mathbf{H}' = \mathbf{AH}$ is equal to column number $\varphi^{-1}(i)$ of $\mathbf{H}$. (No formal proofs are needed, good explanations are enough.)

Solution. Let $\mathbf{H}'$ be the parity-check matrix obtained from $\mathbf{H}$ using the permutation φ. If $\mathbf{H}$ and $\mathbf{H}'$ define the same 1-error-correcting code, then their row spaces are the same. The rows of each of these two matrices constitute a basis for the row spaces. If the rows of $\mathbf{H}$ are $\bar{r}_i$, for $i = 1, 2, \ldots, k$, then, as the rows of $\mathbf{H}$ is a basis for the row space of $\mathbf{H}$, we may conclude that the rows of $\mathbf{H}'$ are

$$\bar{r}'_j = a_{j,1}\bar{r}_1 + a_{j,2}\bar{r}_2 + \cdots + a_{j,k}\bar{r}_k, \qquad j = 1, 2, \ldots, k$$

for elements $a_{i,j} \in Z_2$. This means that

$$\mathbf{H}' = \begin{bmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,k} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,k} \\ \vdots & \vdots & & \vdots \\ a_{k,1} & a_{k,2} & \cdots & a_{k,k} \end{bmatrix} \mathbf{H}$$

As the rows of $\mathbf{H}'$ are linearly independent, it follows that the $k \times k$-matrix above is non-singular, a fact that will be used in the next subproblem.

(c) (2p) Find the number of distinct linear 1-error-correcting codes C of length 15 and size $|C| = 2^{11}$.

Solution. We use the theory behind the lemma of Burnside.

Any parity-check matrix of a code with the given parameters can be obtained from another parity-check matrix by one of the all 15! distinct permutations of the coordinate positions. This because every possible non-zero column appears exactly once in the parity-check matrix. Thus every 1-error-correcting code with the given parameters is contained in the same orbit of 1-error-correcting codes under the group of all 15! permutations of the coordinate positions. It is thus sufficient to count the number N of permutations that fix a 1-error-correcting code C. Then from the theory of Burnside, the number of distinct 1-error-correcting codes with the given parameters is given by $15!/N$.

From the solution of the previous subproblem we know that every permutation φ that fixes a given code C corresponds to a non-singular matrix $\mathbf{A}$ of size 4×4, and vice versa. We count the number of such matrices. The first column can be chosen in 15 ways, as every possible column except the zero column will do. The second column can be any except the zero column or the first column, thus 14 choices. The third cannot belong to the linear span of the first two columns, which contains four columns, thus 12 choices in this case. Finally, the last column can be chosen in $16 - 8 = 8$ distinct ways.

Thus,

ANSWER: The number of distinct 1-error-correcting codes with the given parameters is

$$\frac{15!}{15 \cdot 14 \cdot 12 \cdot 8}.$$

10. (5p) Let $\chi(G)$ denote the chromatic number of a graph G and let $\bar{G}$ denote the complement of G, (so we assume that has no multiple edges or loops). Show that

$$\chi(G) + \chi(\bar{G}) \geq 2\sqrt{n},$$

where n denotes the number of vertices of G.

Solution. Assume that $\chi(G)\chi(\bar{G}) = k$. Then

$$\chi(G) + \chi(\bar{G}) \geq 2\sqrt{k},$$

as the function $x + k/x$ attends its minimum when $x = \sqrt{k}$. It is thus sufficient to prove that $k \geq n$. Assume that $k < n$. Then two vertices a and b will both have the same color in a min coloring of G and in a min coloring of $\bar{G}$. However this is an impossibility as either in G or in $\bar{G}$ there is an edge between a and b.