Matematiska Institutionen
KTH

Soutions to the exam to the course Discrete Mathematics, SF2736, at 14.00 to 19.00 on December 13, 2010.

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 64^{128} is divided by 43.

   Solution: As 43 is a prime number that does not divide 64, we can use the theorem of Fermat:
   $$64^{128} \equiv_{43} 21^{128} \equiv_{43} (21^{42})^3 \cdot 21^2 \equiv_{43} 1^3 \cdot 441 \equiv_{43} 11 \ .$$
   As $0 \leq 11 < 43$ the remainder 11 will be the least positive remainder and thus

   Answer: 11

2. (3p) Draw a graph with 10 vertices and 15 edges that contains a Hamiltonian cycle, but no Eulerian circuit.

   Solution: Draw first a cycle graph consisting of the ten vertices
   $$E = \{1, 2, \ldots, 10\} \ .$$
   Then complete with another five edges between the vertices i and $i + 5$, for $i = 1, 2, \ldots, 5$. The so obtained graph has 10 vertices and 15 edges. The valency of the vertices are 3, and hence no Euler circuit can exist. The original cycle, will be a Hamiltonian cycle.

3. (3p) Find the number of surjective maps f from the set $\{1,2,3,4,5,6\}$ to the set $\{1,2,3,4\}$ with the property that $f(1) \neq f(2)$.

   Solution: The answer will be given by the total number of surjective maps from a set with 6 elements to a set with 4 elements, i.e., $4!S(6,4)$ minus the number of surjective maps from a set with the five elements $\{12,3,4,5,6\}$ to a set with 4 elements, i.e., $4!S(5,4)$. So we have to calculate

   $$4!(S(6,4) - S(5,4)) \ .$$

   We now use the recursion $S(n,k) = S(n-1,k-1) + kS(n-1,k)$.

   $$\begin{array}{rcl} S(6,4) & = & S(5,3) + 4S(5,4) \\ S(5,3) & = & S(4,2) + 3S(4,3) \\ S(4,2) & = & S(3,1) + 2S(3,2) = 1 + 2S(3,2) \\ S(3,2) & = & S(2,1) + 2S(2,2) = 1 + 2 = 3 \\ S(4,3) & = & S(3,2) + 3S(3,3) = 6 \\ S(5,4) & = & S(4,3) + 4S(4,4) = 10 \end{array}$$

   so

   $$S(4,2) = 7 \ , \quad S(5,3) = 7 + 3 \cdot 6 = 25 \ , \quad S(6,4) = 25 + 4 \cdot 10 = 65 \ .$$

   Thus, and finally

   Answer: $24(65-10)$ that is, 1320.

4. (3p) Let G be the group $(Z_{13} \setminus \{0\}, \ \cdot \ )$. Find four non trivial subgroups of G. (You will get 2p if you find just three non trivial subgroups, and 1p if you just find one non trivial subgroup.)

   Solution: We try to get four cyclic subgroups:

   $$< 2 > \quad = \quad \{2,4,8,3,6,12,11,9,5,10,7,1\}$$

   so our first trial gave that 2 generated the full group G, which is one of the two trivial subgroups. Now we get the following four non trivial subgroups:

   $$\begin{array}{rcl} < 2^2 > & = & \{4,3,12,9,10,1\} \\ < 2^3 > & = & \{8,12,5,1\} \\ < 2^4 > & = & \{3,9,1\} \\ < 2^6 > & = & \{12,1\} \end{array}$$

5. (3p) Let p and q be any two odd integers. Show that 2^n divides

   $$\sum_{k=0}^{n} \binom{n}{k} p^k q^{n-k} \ .$$

   Solution: By the binomial theorem

   $$\sum_{k=0}^{n} \binom{n}{k} p^k q^{n-k} = (p+q)^n \ .$$

As both p and q are odd integers we get that $p+q$ is an even integer, i.e.,

$$p+q=2k\ ,$$

for some integer k, and so

$$(p+q)^n=(2k)^n=2^n\cdot k'\ ,$$

where $k'=k^n$.

Part II

6. (3p) Show that every graph on 15 vertices, of which seven have degree (or valency) 3, four have degree 4, three have degree 5 and one has degree 6, must contain at least one cycle.

   Solution: The sum of all valencies is twice the number of edges:

   $$2\cdot|E|=7\cdot 3+4\cdot 4+3\cdot 5+6=58\ .$$

   A graph that does not contain any cycle consists of trees. The number of edges of a tree is less than the number of vertices, so an acyclic graph cannot have more edges than vertices. The above calculation thus shows that the given graph must have a cycle, as the graph has 29 edges and 15 vertices.

7. (4p) Let G be a cyclic group with an odd number of elements and with generator h. Let e denote the identity element of G. Assume that the element g of G satisfies

   $$g^{314}=e \qquad \text{and} \qquad g^{416}=e\ .$$

   Is the above information sufficient to find the element g? If the answer is yes, find the element, otherwise explain why the information is not sufficient.

   Solution: We first find the greatest common divisor of 314 and 416 by using the Euclidian algorithm;

   $$\begin{aligned} 416 &= 314+102 \\ 314 &= 3\cdot 102+8 \\ 102 &= 13\cdot 8-2 \\ 8 &= 4\cdot 2 \end{aligned}$$

   As $\gcd(416,314)=2$ there are integers n and m such that

   $$n\cdot 314+m\cdot 416=2\ .$$

   So

   $$e=e^n\cdot e^m=(g^{314})^n\cdot(g^{416})^m=g^{314n+416m}=g^2\ .$$

   We may thus conclude that the element g has order 2 or 1. However, the order of an element is always a factor in the number of elements of the group. As the number of elements of G is odd, the order of g can not be 2. Thus $g^1=e$, and we may conclude that

   Answer: $g=e$.

8. (4p) Consider the complete graph K_6 on six vertices which are colored with the colors red, green and blue. How many distinct graphs with colored vertices can you obtain from this colored K_6 by deleting two edges.

Solution: There are two cases, either the deleted edges met in one vertex or they do not meet at any vertex.

Case 1: The two deleted edges have no vertex in common. Enumerated the vertex by 1, 2, 3, ..., 6 and assume that after the deletion of edges the vertices 1 and 2 are not neighbors and 3 and 4 are not neighbors. We use the lemma of Burnside and thus consider the group of automorphism of the graph and make the necessary calculations of colorings fixed by the permutations:

$g \in \mathrm{Aut}(Graph)$	$\lvert\mathrm{Fix}(g)\rvert$
(1)(2)(3)(4)(5)(6)	3^6
(1 2)(3)(4)(5)(6)	3^5
(1 2)(3 4)(5)(6)	3^4
(1 2)(3)(4)(5 6)	3^4
(1 2)(3 4)(5 6)	3^3
(1)(2)(3 4)(5)(6)	3^5
(1)(2)(3)(4)(5 6)	3^5
(1)(2)(3 4)(5 6)	3^4
(1 3)(2 4)(5)(6)	3^4
(1 3)(2 4)(5 6)	3^3
(1 4)(2 3)(5)(6)	3^4
(1 4)(2 3)(5 6)	3^3

By the lemma of Burnside the number of colorings in this case will be

$$\frac{1}{12}(3^6 + 3 \cdot 3^5 + 5 \cdot 3^4 + 3 \cdot 3^3) = \frac{8 \cdot 3^5}{12} = 162 \, .$$

Case 2: The two deleted edges had one vertex in common. Denote that vertex by 1 and its deleted vertices by 2 and 3, and the remaining vertices by 4, 5, and 6. Again we use the lemma of Burnside

$g \in \mathrm{Aut}(Graph)$	$\lvert\mathrm{Fix}(g)\rvert$
(1)(2)(3)(4)(5)(6)	3^6
(1)(2)(3)(4 5)(6)	3^5
(1)(2)(3)(4)(5 6)	3^5
(1)(2)(3)(5)(4 6)	3^5
(1)(2)(3)(4 5 6)	3^4
(1)(2)(3)(4 6 5)	3^4
(1)(2 3)(4)(5)(6)	3^5
(1)(2 3)(4 5)(6)	3^4
(1)(2 3)(4)(5 6)	3^4
(1)(2 3)(5)(4 6)	3^4
(1)(2 3)(4 5 6)	3^3
(1)(2 3)(4 6 5)	3^3

By the lemma of Burnside the number of colorings in this case will be

$$\frac{1}{12}(3^6 + 4 \cdot 3^5 + 5 \cdot 3^4 + 2 \cdot 3^3) = \frac{80 \cdot 3^3}{12} = 180 \ .$$

Adding the different possibilities in the two cases we get

Answer: 342.

Remark: An alternative solution can also be given by a direct ”combinatorial” approach, eg by considering the complement of the graph.

Part III

9. A ternary code C of length n is a set of words of length n formed by using letters from the alphabet $\{0, 1, 2\}$. We define the distance between words of length n as the number of positions in which the words differ.

   (a) (2p) Show that the set of words in the code C, where

   $$C = \{0000, 0111, 0222, 1012, 1120, 1201, 2021, 2102, 2210\} \ ,$$

   has the property that every possible ternary word of length 4 is at distance at most one from a unique word of C.

   Solution: The number of words in any 1-sphere with center in a code word $\bar{c}$ will be

   $$|\mathrm{S}_1(\bar{c})| = 1 + 2 \cdot \binom{4}{1} = 1 + 2 \cdot 4 = 9 \ .$$

   By inspection we note that the minimum distance in C is 3. Consequently, the 1-spheres with centers in code words will be mutually disjoint, and thus

   $$|\bigcup_{\bar{c} \in C} \mathrm{S}_1(\bar{c})| = \sum_{\bar{c} \in C} |\mathrm{S}_1(\bar{c})| = \sum_{\bar{c} \in C} 9 = |C| \cdot 9 = 81 = 3^4 \ .$$

   As there are in total 3^4 ternary words of length 4, we get that every ternary word of length 4 can uniquely be corrected to a code word.

   (b) (4p) Find, and describe in a suitable way, another ternary code C of some length $n \geq 5$ that has the property that every possible ternary word of length n is at distance at most one from a unique word of C.

   Solution: In general, a 1-sphere in the space Z_3^n, the set of ternary words of length n, will be of size

   $$|\mathrm{S}_1(\bar{c})| = 1 + 2 \cdot \binom{n}{1} = 1 + 2n \ .$$

   For a code with the desired properties, spheres with centers at code words shall partition the set of all 3^n words into mutually disjoint sets of size $1 + 2n$, so

$1+2n$ must divide 3^n and the minimum distance of the code must be 3. It is easy to see that $1+2n$ is a power of 3 if for example $n = 13$.

So we will try to construct a such closed packed ternary 1-error correcting code C of length 13. The number of words of C will be

$$|C| = \frac{3^{13}}{|\mathrm{S}_1(\bar{c})|} = \frac{3^{13}}{3^3} = 3^{10} .$$

We will define C as the null space of a ternary matrix H. As $|C| = 3^{10}$ we conclude that C must have dimension 10 over the field Z_3, and by the fundamental theorem of linear algebra H will be an 3×13-matrix of rank 3.

We produce the matrix H in the same way as in the binary case, but we must be sure that no two words differ in 2 (or 1) positions. Thus no column of H can be a multiple of another column, and as in the binary case, H cannot contain the all zero column. So a bit trial and error gives the following matrix:

$$H = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 1 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \end{bmatrix}$$

Answer: A suitable code would for example be the null space of the above matrix H.

10. (4p) Let $\mathcal{S}_n$ denote the set of permutations on a set with n elements, and let p be a prime number less than or equal to n. Derive a formula for the number of solutions $\varphi \in \mathcal{S}_n$ to the equation

$$\varphi^p = \mathrm{id}.$$

Solution: Let φ be any permutation such that $\varphi^p = \mathrm{id}$. Then the order of φ divides p and thus as p is a prime, the order of φ must be the prime p.

It is well known that the order of a permutation is the least common multiple of the length of the cycles when the permutation is considered as a product of mutually disjoint cycles. So again using the fact that p is a prime, we get that if φ has order p, then φ will be a product of a number mutually disjoint cycles of length p and cycles of length 1.

Every choice of p elements will give $(p-1)!$ distinct cycles, as we can fix one of the p chosen elements to the p-cycles, e.g., the "smallest" element, and then get $(p-1)!$ different cycles according to in which order the remaining $p-1$ of the chosen p elements are. Furthermore, as the p-cycles that occur in the permutation φ are not labeled, we get that the number of permutations with k mutually disjoint p-cycles will be

$$\frac{1}{k!} \cdot \binom{n}{p, p, \ldots, p, n-kp} \cdot ((p-1)!)^k = \frac{n! \cdot ((p-1)!)^k}{k! \cdot (p!)^k (n-kp)!} = \frac{n!}{k! \cdot p^k \cdot (n-kp)!} ,$$

as the multinomial coefficient gives the number of ways to choose k labeled subsets of size p and the fraction $1/k!$ compensates for the labeling. So summing and regarding that also $\mathrm{id.}^p = \mathrm{id}$ we get the

Answer:

$$1+\sum_{1\le k\le n/p}\frac{n!}{k!\cdot p^k\cdot(n-kp)!}\ .$$