VO Discrete Mathematics – VU Diskrete Mathematik

Exercises for Oct 10/11/15, 2012

1) A simple undirected graph is called cubic if each of its vertices has degree 3.

(a) Find a cubic graph with 6 vertices!

(b) Is there a cubic graph with an odd number of vertices?

(c) Prove that for all $n \geq 2$ there exists a cubic graph with $2n$ vertices!

2) Use a suitable graph theoretical model to solve the following problems:

(a) Show that in every city at least two of its inhabitants have the same number of neighbours!

(b) 7 friends want to send postcards according to the following rules: (i) Each person sends and receives exactly 3 cards. (ii) Each one receives only cards from those to whom he or she sent a card.

Tell how this can be done or prove that this is impossible!

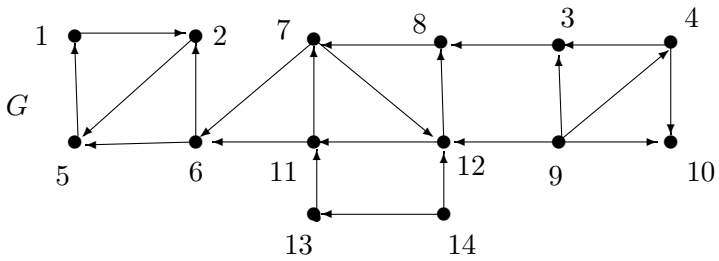
3) Show that each of the following statements is equivalent to the statement „T is a tree“:

1. Every two nodes of T are connected by exactly one path.
2. T is connected and $\alpha_0(T) = \alpha_1(T) + 1$.
3. T is a minimal connected graph, i.e., deleting an edge destroys connectivity.
4. T is a maximal acyclic graph, i.e., adding an edge generates a cycle.

4) Let $G = (V, E)$ be a simple and undirected graph with $|V| > 4$. The complement $G^\kappa = (V^\kappa, E^\kappa)$ of G is defined as follows: $V^\kappa = V$ and $vw \in E^\kappa$ if and only if $vw \notin E$. Show that either G or G^κ (or both) must contain a cycle! Furthermore, determine all trees T such that T^κ is a tree as well!

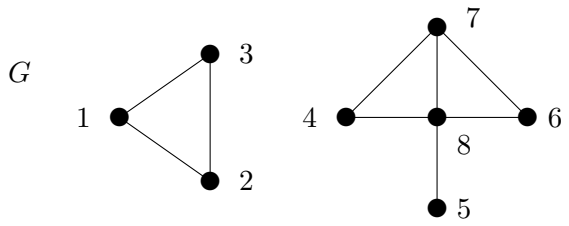
5) Let $G = (V, E)$ be a simple and undirected graph with $V = \{v_1, \ldots, v_n\}$. Its adjacency matrix is denoted by $A = (a_{ij})_{1 \leq i,j \leq n}$. Moreover, let $A^k = (a_{ij}^{[k]})_{1 \leq i,j \leq n}$ be the k-th power of A. Prove that $a_{ij}^{[k]}$ equals the number of walks from v_i to v_j having length k!

6) Find the strong connected components and the reduction G_R of the graph G below. Furthermore, determine all node bases of G.



7) Let $G = (V, E)$ be a simple and directed graph and G_R its reduction. Prove that G_R is acyclic!

8) Use the matrix tree theorem to compute the number of spanning forests of the graph below!



9) K_n denotes the complete graph with n vertices. Show that the number of spanning trees of K_n is n^{n-2}!

Hint: Use the matrix tree theorem and delete the first column and the first row of $D(K_n) - A(K_n)$. Then add all rows (except the first) to the first one and observe that all entries of the new first row are equal to 1. Use the new first row to transform the matrix in such a way that the submatrix built of the second to the last row and second to the last column is diagonal matrix.

10) If T is a tree having no vertex of degree 2, then T has more leaves than internal nodes. Prove this claim

(a) by induction,

(b) by considering the average degree and using the handshaking lemma.

UE Discrete Mathematics – VU Diskrete Mathematik

Exercises for Oct 17/18/22, 2012

11) Let $G = (V, E)$ be a connected graph with an even number of vertices. Show that there is a (not necessarily connected) spanning subgraph (i.e. a subgraph with vertex set V) in which all vertices have odd degree. Is this also true for non-connected graphs?

12) Prove: If $M = (E, S)$ is a matroid and A and B are two bases (i.e., maximal independent sets) of M, then $|A| = |B|$.

13) Let $M = (E, S)$ be a matroid and $\mathcal{B}$ the family of all its bases. Let $A, B \in \mathcal{B}$ such that $A \neq B$. Prove that

(a) neither of the inclusions $A \subseteq B$ and $B \subseteq A$ holds,

(b) for each $x \in A$ there exists $y \in B$ such that $(A \setminus \{x\}) \cup \{y\} \in \mathcal{B}$.

Hint: Show first that, if $x \in A \cap B$ in (b), then by (a) we must have $y = x$, and if $x \in A \setminus B$, then we must have $y \in B \setminus A$.

14) Let $\mathcal{B}$ be a family of sets which satisfies (a) and (b) of the previous exercise. Show that there is a matroid having $\mathcal{B}$ as its family of all its bases.

15) Let $G = (V, E)$ be an undirected graph. Set $M_k(G) = (E, S)$ where

$$S = \{A \subseteq E \mid A = F \cup M \text{ where } F \text{ is a forest and } |M| \leq k\}.$$

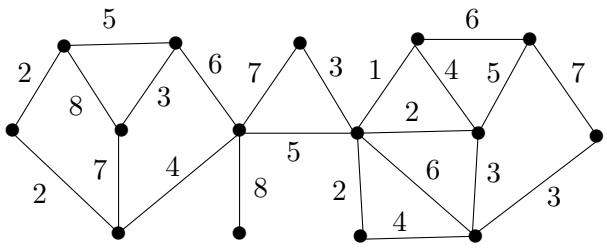
Prove that $M_k(G)$ is a matroid.

16) Let $M = (E, S)$ be a matroid and $A \subseteq E$. The rank $r(A)$ of A is defined as the cardinality of a maximal independent subset of A. Prove that for all $A, B \subseteq E$ we have

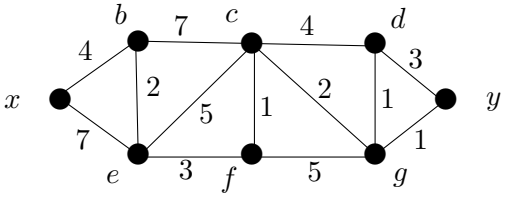
(a) $r(A) \leq |A|$, (b) $A \subseteq B$ implies $r(A) \leq r(B)$, (c) $r(A \cap B) + r(A \cup B) \leq r(A) + r(B)$.

17) Use Kruskal's algorithm to find a minimal and a maximal spanning tree of the following weighted graph.

H

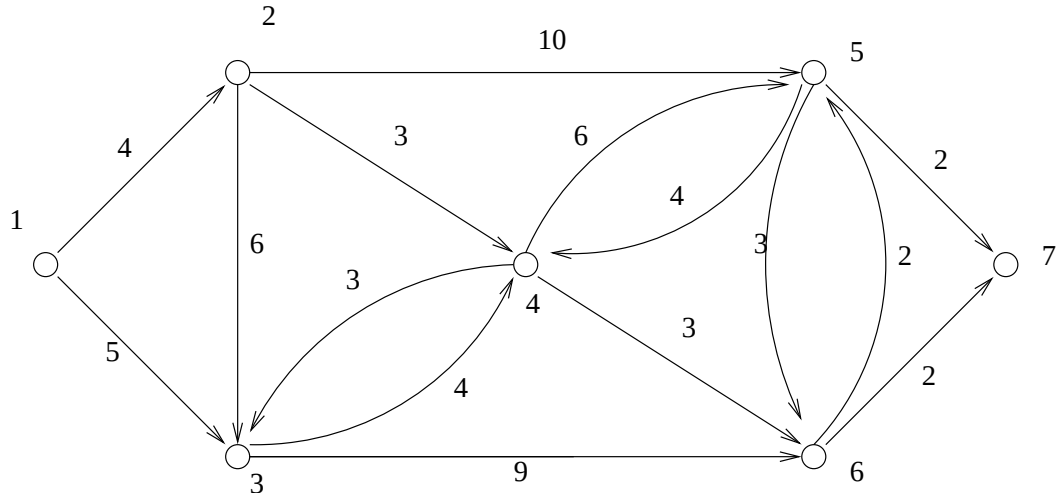


18) Use Dijkstra's algorithm to determine $d(x, y)$ in the following graph.



19) Use one of the algorithms presented in the lecture to construct a spanning tree which contains all the shortest paths connecting vertex x with all the other vertices in the graph of Exercise 18.

20) Use the algorithm of Floyd-Warshall to compute all distances in the following graph.



UE Discrete Mathematics – VU Diskrete Mathematik

Exercises for Oct 24/ 25/ 29 2012

21) Find a graph $G = (V, E)$ and two vertices $x, y \in V$ such that Dijkstra's algorithm does not compute the distance $d(x, y)$ correctly.

22) The matrix W corresponds to the weight function w of flow network $G = (V, E, w, s, t)$ and the matrix $\mathbf{\Phi}$ to a flow ϕ on G.

$$W = \begin{pmatrix} 0 & 5 & 7 & 8 & 0 & 0 & 0 \\ 0 & 0 & 4 & 0 & 10 & 0 & 0 \\ 0 & 0 & 0 & 5 & 3 & 11 & 0 \\ 0 & 0 & 0 & 0 & 0 & 6 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 9 \\ 0 & 0 & 0 & 0 & 0 & 0 & 4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \qquad \mathbf{\Phi} = \begin{pmatrix} 0 & 5 & 6 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 5 & 0 & 0 \\ 0 & 0 & 0 & 1 & 2 & 3 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 7 \\ 0 & 0 & 0 & 0 & 0 & 0 & 4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

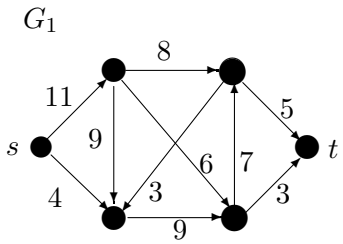
(a) Determine $v(\phi)$.

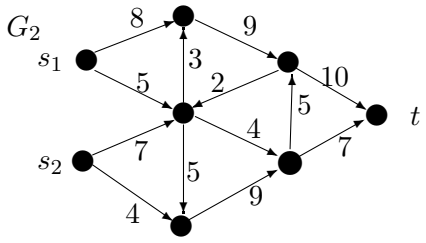
(b) Find an augmenting path comprising forward edges only and an augmenting path with at least one backward edge.

(c) Find a minimal cut.

(d) Find a maximal flow on G.

23) Use the algorithm of Ford and Fulkerson to compute a maximal flow in the network G_1 below!





24) Use the algorithm of Ford and Fulkerson to compute a maximal flow in the network G_2 which has two sources s_1 and s_2!

25) For a simple and undirected graph G we define the *line graph* $\bar{G}$ as follows: $V(\bar{G}) = E(G)$ and $(e, f) \in E(\bar{G})$ if and only if the edges e and f share a vertex. Prove that the line graph of an Eulerian graph is Eulerian and Hamiltonian!

26) Let G_n denote the n-dimensional hypercube. Show that G_n is Hamiltonian if $n \geq 2$.

27) Prove that a graph G is bipartite if and only if each cycle in G has even length.

28) Construct a schedule for the matches in a league of $2n$ teams which meets the following constraints:

(a) In each round each team plays exactly one match.

(b) In the end each team must have played against each of the other teams exactly once.

Hint: Consider the graph K_{2n} on the vertex set $\{1, 2, \ldots, 2n\}$ and show that each of the sets $M_i = \{1i\} \cup \{xy \mid x + y \equiv 2i \mod 2n - 1 \text{ and } x \neq y,\ x \neq 1,\ y \neq 1\}$ is a perfect matching (for $i = 2, \ldots, 2n$).

29) Let M be a matching of a simple and undirected graph $G = (V, W)$. A path W in G is called alternating if exactly every other edge of W is in M. We call an alternating path extending if the start as well as the end vertex of W is not incident with any $e \in M$. Prove: If W is an extending alternating path, then $M \triangle W := (M \setminus W) \cup (W \setminus M)$ is a matching and $|M \triangle W| = |M| + 1$.

30) Show the following inequality for Ramsey numbers: If $r \geq 3$ then

$$R(n_1, \ldots, n_{r-2}, n_{r-1}, n_r) \leq R(n_1, \ldots, n_{r-2}, R(n_{r-1}, n_r))$$

Hint: Let $n = R(n_1, \ldots, n_{r-2}, R(n_{r-1}, n_r))$ and consider an edge colouring of K_n with r colours, say $c_1, \ldots, c_r$. Identify the colours c_{r-1} and c_r and apply the Ramsey property for $r - 1$ colours.

UE Discrete Mathematics

Exercises for Nov 7/8, 2012

31) In how many ways can the letters a, a, b, b, c, d, e be listed such that the letter c and d are not in consecutive positions?

32) Let M be a non-empty set. Show that M has as many subsets with an odd number of elements as subsets with an even number of elements.

33) Find the number of ways to place n rooks on an $n \times n$ chess board such that no two of them attack each other.

34) Let n be a positive integer and let $(a_1, \ldots, a_n)$ be a permutation of $\{1, 2, \ldots, n\}$. Define

$$A_k = \{a_i \mid a_i < a_k, i > k\} \text{ and } B_k = \{a_i \mid a_i > a_k, i < k\}$$

for $1 \leq k \leq n$. Prove that $\sum_{k=1}^{n} |A_k| = \sum_{k=1}^{n} |B_k|$.

35) Let A be a set of 11 positive integers such that for all $x \in A$ we have $20 \not| x$. Prove that there are two integers $a, b \in A$ such that $20|(a+b)$ or $20|(a-b)$.

36) Let $A = \{1, 2, 3, 4\}$ and $B = \{1, 2, \ldots, 82\}$. All points of the plane having coordinates (x, y) which satisfy $(x, y) \in A \times B$ are coloured with one of the colours red, green or blue. Prove that there exists a monochromatic rectangle.

Remark: A rectangle is called monochromatic if all its four vertices have the same colour.

37) Let $n \in \mathbb{N}$. Prove the identities

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k} \qquad \text{and} \qquad \sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}$$

by using only the combinatorial interpretation of the binomial coefficients.

38) Let $n \in \mathbb{N}$. Prove the identity

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

39) Prove that for all complex number x and all $k \in \mathbb{N}$ we have

$$\binom{-x}{k} = (-1)^k \binom{x+k-1}{k}.$$

40) Compute the number of words made of $2n$ letters taken from the alphabet $\{a_1, a_2, \ldots, a_n\}$ such that each letter occurs exactly twice and no two consecutive letters are equal.

UE Discrete Mathematics

Exercises for Nov 14/22, 2012

41) Let

$$f_n = |\{\pi \in S_n \mid \forall 1 \leq i \leq n : \pi(i) \neq i\}|.$$

Prove that $f_1 = 0$, $f_2 = 1$ and $f_n = (n-1)(f_{n-1} + f_{n-2})$. Furthermore, prove that this recurrence relation implies

$$f_n = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}.$$

42) Prove the following identity:

$$x^n = \sum_{k=0}^{n} S_{n,k}(x)_k \qquad (n \geq 0).$$

43) Let A, B be two finite sets with $|A| = n$ and $|B| = k$. How many injective mappings $f : A \to B$ are there? Furthermore, show that the number of surjective mappings $f : A \to B$ equals $k!S_{n,k}$.

44) The n-th Bell number equals the number of set partitions of $\{1, 2, \ldots, n\}$. We set $B_0 := 1$. Prove the following identities:

$$B_n = \sum_{k=0}^{n} S_{n,k} \qquad \text{and} \qquad B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} B_k.$$

45) Compute $\sum_{k=1}^{n-1} \frac{1}{k(n-k)}$ in two ways: (a) using a term by term partial fraction decomposition, (b) with generating functions.

46) Use generating functions to answer the following question: What is the number of solutions of the equation $a + b + c + d = 25$ if $a, b, c, d \in \{0, 1, 2, \ldots, 9\}$?

47) Solve the following recurrence using generating functions: $a_{n+1} = 2a_n - 3$, $a_0 = 1$.

48) Solve the following recurrence using generating functions: $a_{n+1} = a_n + (n+1)^2$.

49) Solve the following recurrence using generating functions: $a_{n+2} = 3a_{n+1} - 2a_n$, $a_0 = 1$, $a_1 = 3$.

50) Let a_n denote the number of fat subsets of $\{1, 2, \ldots, n\}$ where a set A is called *fat* if $A = \emptyset$ or $\forall k \in A : k \geq |A|$. Prove that $a_n = F_{n+2}$ (as usual $(F_n)_{n \geq 0}$ denotes the sequence of the Fibonacci numbers) and show that this implies

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

UE Discrete Mathematics

Exercises for Nov 21/29, 2012

51) Use generating functions to find a closed form expressions for the sum $\sum_{k=0}^{n}(k^2+3k+2)$.

52) Compute

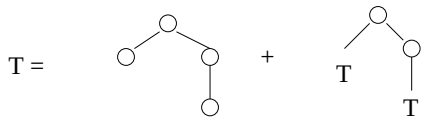
$$[z^n]\frac{2+3z^2}{\sqrt{1-5z}}.$$

53) Prove the following identity:

$$\sum_{n\geq 0}\binom{2n}{n}z^n=\frac{1}{\sqrt{1-4z}}.$$

54) A t-ary tree is a plane rooted tree such that every node has either t or 0 succesors. A node with t succesors is called internal nodes. How many leaves has a t-ary tree with n internal nodes? Moreover, let a_n be the number of t-ary trees with n internal nodes and $A(z)$ the generating function of this sequence. Find a functional equation for $A(z)$!

55) Compute the numbers t_n of plane rooted trees with n nodes which can be described by the equation



56) Compute the number of plane rooted trees with n nodes.

57) Consider a regular $(n+2)$-gon A, say, with the vertices $0,1\ldots,n+1$. A triangulation is a decomposition of A into n triangles such that the 3 vertices of each triangle are vertices of A as well. Show that the set $\mathcal{T}$ of triangulations of regular polygons can be described as a combinatorial construction satisfying

$$\mathcal{T}=\{\varepsilon\}\cup\mathcal{T}\times\Delta\times\mathcal{T}$$

where Δ denotes a single triangle **and ε denotes the empty triangulation (consisting of no triangle and corresponding to the case $n=0$)**. What is the number of triangulations of A?

58) Let $\mathcal{L}$ denote the set of words over the alphabet $\{a,b\}$ that contain exactly k occurrences of b. Obviously, the number of words in $\mathcal{L}$ which have exactly n letters is $\binom{n}{k}$. Prove this by finding a specification of $\mathcal{L}$ as combinatorial construction and translating this specification into generating functions.

59) Let $\mathcal{L}^{[d]}$ denote the set of words over the alphabet $\{a,b\}$ that contain exactly k occurrences of b such that there are always never more than d a's between two consecutive b's. Find a specification of $\mathcal{L}^{[d]}$ as combinatorial construction and use generating functions to compute the number of words in $\mathcal{L}^{[d]}$ having exactly n letters.
Remark: The result is an alternating sum which cannot be simplified further.

60) Let s_{nk} be the Stirling numbers of the first kind, that is, the number of permutations of $\{1, 2, \ldots, n\}$, where the cycle representation has exactly k cycles. Prove

$$\sum_{n,k} s_{nk} \frac{z^n}{n!} u^k = e^{u \log \frac{1}{1-z}} = \frac{1}{(1-z)^u}.$$

Remark: Start with the identity

$$\sum_{k=0}^{n} s_{nk} u^k = u(u+1)(u+2)\ldots(u+n-1).$$

UE Discrete Mathematics

Exercises for Nov 28/Dec 6, 2012

61) Use exponential generating functions to determine the number a_n of of ordered choices of n balls such that there are 2 or 4 red balls, an even number of green balls and an arbitrary number of blue balls.

62) An involution is a permutation π such that $\pi \circ \pi = \mathrm{id}_M$ where $M = \{1, 2, \ldots, n\}$. Let $\mathcal{I}$ be the set of involutions. Determine the exponential generating function $I(z)$ of $\mathcal{I}$.

63) Show the following formula for the Stirling numbers of the first kind (with the help of a proper labelled combinatorial construction):

$$\sum_{n,k} s_{nk} \frac{z^n}{n!} u^k = e^{u \log \frac{1}{1-z}} = \frac{1}{(1-z)^u}.$$

64) Show the following formula for the Stirling numbers of the second kind:

$$\sum_{n,k} S_{nk} \frac{z^n}{n!} u^k = e^{u(e^z - 1)}.$$

65) Prove the following representation for the Stirling numbers of the second kind:

$$S_{nk} = \frac{1}{k!} \sum_{j=0}^{k} (-1)^{k-j} \binom{k}{j} j^n.$$

Remark. Compute first the generating function for $\sum_n S_{nk} z^n/n! = (e^z - 1)^k/k!$.

66) Let P be the set of all divisors of 12. Determine the Möbius function of $(P, |)$.

67) Let $(P, \leq)$ be the poset defined by $P = \{0, 1, 2, 3, 4\}$ and $0 \leq 1 \leq 4,\ 0 \leq 2 \leq 4,\ 0 \leq 3 \leq 4$. Compute all values $\mu(x, y)$ for $x, y \in P$.

68) Let $(P_1, \leq_1)$ and $(P_2, \leq_2)$ be two locally finite posets and $(P, \leq)$ be defined by $P = P_1 \times P_2$ and for $(a, x), (b, y) \in P$:

$$(a, x) \leq (b, y) \iff a \leq_1 b \wedge x \leq_2 y.$$

Show that $(P, \leq)$ is a poset and that the Möbius functions of P, P_1, P_2 satisfy $\mu_P((a, x), (b, y)) = \mu_{P_1}(a, b) \cdot \mu_{P_2}(x, y)$.

69) Draw the Hasse diagram of $(2^{\{1,2,3\}}, \supseteq)$ and redo the proof of the principle of inclusion and exclusion for the special case of three sets $A_1, A_2, A_3 \subseteq M$. Carry out every step in detail.

70) Let p, q, r be three distinct prime numbers and $m = pqr$. How many of the numbers $1, 2, \ldots, m$ are relatively prime to m? (Two numbers x and y are called relatively prime if their greatest common divisor is 1.)

UE Discrete Mathematics

Exercises for Dec 5/13, 2012

71) Prove the following assertions:

(a) Every finite lattice has a 0-element and a 1-element.

(b) In every lattice L we have $(x \wedge y) \vee y = y$ for all $x, y \in L$

(c) There exist a lattice such that the following implication is not true:

$$x \leq z \implies \forall y : x \vee (y \wedge z) = (x \vee y) \wedge z.$$

72) Let $(P, \leq)$ be a finite poset. A subset $C \subseteq P$ is called a *chain* if $(C, \leq)$ is a linearly ordered set. A subset $A \subseteq P$ is called an *antichain* if no two elements of A are comparable with respect to $\leq$. A *chain cover* of P is a partition $P = C_1 \cup C_2 \cup \cdots \cup C_k$ in which all the C_i are chains. Dilworth's Theorem asserts that the size of any largest antichain is equal to the number of chains in a smallest chain cover.
Use Dilworth's Theorem to prove that every poset with at least $rs+1$ elements has either a chain with $r+1$ elements or an antichain with $s+1$ elements.

73) Let a, b, c be integers. Prove: If $a \mid b$ and $a \mid c$, then for all integers x, y we have $a \mid (xb + yc)$.

74) Prove: If x and y are odd integers, then $2 \mid (x^2 + y^2)$ but $4 \nmid (x^2 + y^2)$.

75) Prove that for every integer n the number $n^2 - n$ is even and that $n^3 - n$ is a multiple of 6.

76) Consider two integers a and b such that $\gcd(a, 4) = 2$ and $\gcd(b, 4) = 2$. Prove that then $\gcd(a + b, 4) = 4$.

77) Prove that any two positive integers a, b satisfy $\gcd(a, b) \cdot \mathrm{lcm}(a, b) = a \cdot b$.

78) Use the Euklidean algorithm to find two integers a and b such that $2863a + 1057b = 42$.

79) Use the Euklidean algorithm to find all greatest common divisors of $x^3 + 5x^2 + 7x + 3$ and $x^3 + x^2 - 5x + 3$ in $\mathbb{Q}[x]$.

80) Prove that there exist infinitely many prime numbers p which are solutions of the equation $p \equiv 3 \mod 4$.

Hint: Assume that there are only finitely many such primes, say $p_1, \ldots, p_n$, and consider the number $4p_1p_2 \cdots p_n - 1$.

UE Discrete Mathematics

Exercises for Dec 12/20, 2012

81) Find (without using a computer) the last two digits of 2^{1000}.

82) Prove that none of the integers $n^4 + 4^n$, where $n > 1$, is a prime number.

Hint: Consider the cases n even and n odd. In particular, if n is odd, consider the decomposition $(n^2 + 2^n + n2^{(n+1)/2})(n^2 + 2^n - n2^{(n+1)/2})$.

83) Prove or disprove:

(a) If $\gcd(a, b) = 1$ then $\gcd(a^2, ab, b^2) = 1$.

(b) If $a^2 \mid b^3$ then $a \mid b$.

84) Use the Chinese remainder theorem to solve the following system of congruence relations:

$$\begin{aligned} 3x &\equiv 12\ (13) \\ 5x &\equiv 7\ (22) \\ 2x &\equiv 3\ (7) \end{aligned}$$

85) Use the Chinese remainder theorem to solve the following system of congruence relations:

$$\begin{aligned} 5x &\equiv 8\ (32) \\ 14x &\equiv 2\ (22) \\ 9x &\equiv 3\ (15) \end{aligned}$$

86) Prove: If a prime number p satisfies $\gcd(a, p-1) = 1$, then for every integer b the congruence relation $x^a \equiv b(p)$ has a solution.

87) Let $(n, e) = (3233, 49)$ be a public RSA key. Compute the decryption key d.

88) Use the key of exercise 87) to encrypt the string „`COMPUTER`“. Decompose the string into blocks of length 2 and apply the mapping `A` $\mapsto 01$, `B` $\mapsto 02, \ldots,$ `Z` $\mapsto 26$.

89) Prove that the identity

$$\varphi(m \cdot n) = \varphi(m)\varphi(n)\frac{\gcd(m, n)}{\varphi(\gcd(m, n))}$$

holds for all $m, n \in \mathbb{N}^+$. φ denotes Euler's totient function.

90) Consider an RSA cryptosystem with $n = pq$, p and q being odd primes with $p \neq q$. Let $N_{p,q}$ denote the number of possible pairs (e, d) such that (e, n) and (d, n) are the public and private key, respectively. Show that $N_{p,q} = \varphi(\lambda(n))$, where λ is the Carmichael function and φ Euler's totient function, and that $2 \leq N_{p,q} < \lambda(n)/2$.

UE Discrete Mathematics

Exercises for Dec 19 2012/Jan 10, 2013

91) Let (e, n) and (d, n) be Bob's public and private RSA key, respectively. Suppose that Bob sends an encrypted message c and Alice wants to find out the original message m. She has the idea to send Bob a message and ask him to sign it. How can she find out m?

Hint: Pick a random integer r and consider the message $r^e c \mod n$.

92) Let G be a finite group and $a \in G$ an element for which $\mathrm{ord}_G(a)$ is maximal. Prove that for all $b \in G$ the order $\mathrm{ord}_G(b)$ is a divisor of $\mathrm{ord}_G(a)$.

93) Show that $m \mid n$ implies $\lambda(m) \mid \lambda(n)$ where λ denotes the Carmichael function.

Hint: Prove first that $a_i \mid b_i$ for $i = 1, \ldots, k$ implies $\mathrm{lcm}(a_1, a_2, \ldots, a_k) \mid \mathrm{lcm}(b_1, b_2, \ldots, b_k)$.

94) List all irreducible polynomials up to degree 3 in $\mathbb{Z}_3$.

95) Decompose $x^4 + x^3 + 1$ into irreducible factors over $\mathbb{Z}_2$.

96) Let K be a field and $p(x) \in K[x]$ a polynomial of degree m. Prove that $p(x)$ cannot have more than m zeros (counted with multiplicities).

Hint: Use the fact that $K[x]$ is a factorial ring.

97) Let R be a ring and $(I_j)_{j \in J}$ be a family of ideals of R. Prove that $\bigcap_{j \in J} I_j$ is an ideal of R.

98) Let R be a ring and I an ideal of R. Then $(R/I, +)$ is the factor group of $(R, +)$ over $(I, +)$. Define a multiplication on R/I by

$$(a + I) \cdot (b + I) := (ab) + I.$$

Prove that this operation is well defined, i.e. that

$$\left.\begin{array}{rl} & a + I = c + I \\ \text{and} & b + I = d + I \end{array}\right\} \implies (ab) + I = (cd) + I.$$

Furthermore, show that $(R/I, +, \cdot)$ is a ring.

99) Let $U = \{\bar{0}, \bar{2}, \bar{4}\} \subseteq \mathbb{Z}_6$. Show that U is an ideal of $(\mathbb{Z}_6, +, \cdot)$. Is it a subring as well? Does it have a 1-element?

100) Show that $(\mathbb{Z}[x], +, \cdot)$ is a ring and that $1 \notin (\{x, x + 2\})$.

Remark: It can be shown that a principal ideal which is generated by $a_1, a_2, \ldots, a_k$ can be alternatively generated by $\gcd(a_1, a_2, \ldots, a_k)$. Therefore this example shows that $\mathbb{Z}[x]$ is a ring where not every ideal is a principal ideal. As a consequence, $\mathbb{Z}[x]$ cannot be a Euklidean ring.

UE Discrete Mathematics

Exercises for Jan 9/17, 2013

101) Show that the set $\{a+b\sqrt{2} \mid a,b \in \mathbb{Q}\}$ with the usual addition and multiplication is a field. Compute $(3-5\sqrt{2})^{-1}$.

102) Show that the set $R = \{a+b\sqrt{2} \mid a,b \in \mathbb{Z}\}$ with the usual addition and multiplication is an integral domain but not a field. Furthermore, prove that there are infinitely many units in R and give three concrete examples.

103) Find all irreducible Polynomials of $\mathbb{R}[x]$

Hint: Note that if a polynomial $p(x) \in \mathbb{R}[x]$ has a complex zero $a+bi$, then its conjugate $a-bi$ is a zero of $p(x)$, too. Use this fact to conclude that every polynomial of degree at least 3 in $\mathbb{R}[x]$ is reducible.

104) Give a reason why the Chinese remainder theorem (suitably modified) can be applied to the following system of congruence relations over $\mathbb{Q}[x]$ and use it to solve the system.

$$\begin{aligned}(x+1)P(x) &\equiv 2x+1 \ (x^2+x+1)\\ (x+2)P(x) &\equiv 3x+3 \ (x^2+2x+3)\end{aligned}$$

105) If $(R,+,\cdot)$ is a ring and I_1, I_2 two of its ideals, then

$$\begin{aligned}I_1 + I_2 :=& \{a+b \mid a \in I_1, b \in I_2\}, \text{ and}\\ I_1 * I_2 :=& \{a_1b_1 + a_2b_2 + \cdots + a_nb_n \mid n \geq 1, a_i \in I_1, b_i \in I_2 \text{ for } 1 \leq i \leq n\}\end{aligned}$$

are ideals as well.

106) Show that $\sqrt{2}+\sqrt{3}$ is algebraic over $\mathbb{Q}$ and determine its minimal polynomial.

107) Show that $\sqrt{3}+i$ is algebraic over $\mathbb{Q}$ and determine its minimal polynomial.

108) Let K be a field. Prove:

(a) If $a,b \in K$, then for all $k,l \in \mathbb{N}^+$ the element $\sqrt[k]{a}\sqrt[l]{b}$ is algebraic over K.

(b) If a is algebraic over K, then for all $n \in \mathbb{N}^+$ the element $\sqrt[n]{a}$ is algebraic over K as well.

109) Which of the following polynomials is primitive over $\mathbb{Z}_3$?

$$x^3+x^2+x+1, \quad x^3+x^2+x+2, \quad x^3+2x+1.$$

110) Show that $p(x) = x^6+x^5+x^2+x+1$ is a primitive polynomial over $\mathbb{Z}_2$.

UE Discrete Mathematics

Exercises for Jan 16/24, 2013

111) Let K be a field with $\mathrm{char}(K) = p$. Prove that $(a+b)^p = a^p + b^p$ for all $a, b \in K$.

Hint: Use the binomial theorem and consider the equation $\binom{p}{k} = p \cdot \frac{(p-1)!}{k!(p-k)!}$ for $0 < k < p$. Show that $\binom{p}{k} \in \mathbb{N}$ implies that the fraction on the right-hand side must be an integer, too, since the factors in the denominator do not divide p.

112) Construct a field with 8 elements and demonstrate on some concrete examples how addition and multiplication are done in this field.

113) Consider the field $\mathbb{Z}_2[x]/(m(x))$ where $m(x) = x^8 + x^4 + x^3 + x + 1$. Hence the residue classes modulo $m(x)$ are

$$\overline{b(x)} = \overline{b_7 x^7 + b_6 x^6 + \cdots + b_1 x + b_0}$$

and can be identified with a byte $b_7 b_6 \cdots b_1 b_0$. Compute the sum of the two bytes 10010101 and 11001100 in this field.

114) Consider again the field $\mathbb{Z}_2[x]/(m(x)) = \mathbb{F}_{256}$ and define the mapping $S : \mathbb{F}_{256} \to \mathbb{F}_{256}$ by set $S(y) = 1/y$ (for $y \neq 0$) and $S(0) = 0$. Compute $S(10010101)$ and show (with the help of an example) that $S(y_1 + y_2)$ does not coincide with $S(y_1) + S(y_2)$.

115) The only irreducible polynomials of degree 3 over $\mathbb{Z}_2$ are $f(x) = x^3 + x^2 + 1$ and $g(x) = x^3 + x + 1$. Let α be a zero of $f(x)$ and β be a zero of $g(x)$. Then $\mathbb{Z}_2(\alpha)$ and $\mathbb{Z}_2(\beta)$ are fields with 8 elements. Prove that these two fields are isomorphic.

116) Consider a linear code with generator matrix

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 \end{pmatrix}$$

Compute a check matrix H and a correction scheme (with the help of the syndomes $S_H(v) = vH^T$). What is the minimum distance of this code?

117) Let $g(x) = x^3 + x^2 + 1$ the generating polynomial of a polynomial code over $\mathbb{F}_2$ that induces as $(6,3)$-linear code, that is, polynomials $p(x)$ of degree smaller than 3 are encoded by $f(p(x)) = p(x)g(x)$ to a polynomial of degree smaller than 6. Compute the corresponding generator matrix G. Furthermore, choose a check polynomial $h(x)$ of degree 3 and compute (with the help of $h(x)$) a correction scheme.

118) Let a (n,k)-linear code $C \subseteq \mathbb{F}_q^n$ be given by its generator matrix G. The dual code C^* of C is defined by

$$C^* = \{x \in \mathbb{F}_q^n : x \cdot c = 0 \text{ for all } c \in C\}.$$

Show that C^* is generated by the check matrix H of C and is, thus, a $(n, n-k)$-linear code.

119) Compute the dual code C^* of a linear code C that is represented by

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

120) Let $(s_n)_{n\geq 0}$ be a linear recurrence sequence (of order k) over a finite field $\mathbb{F}_q$:

$$s_{n+k} = a_0 s_n + a_1 s_{n+1} + \cdots a_{k-1} s_{n+k-1},$$

where $a_0, \ldots, a_{k-1} \in \mathbb{F}_q$ are fixed and $s_0, \ldots, s_{k-1}$ are given. Show that $(s_n)_{n\geq 0}$ has to be a periodic sequence.