DMG – exam

Rules

- The time limit is 120 minutes.
- The maximal gain is 80 points.
- Allowed is having a pen, a paper, and an ordinary calculator. It is not allowed to use a cell phone, a computer, or a programmable calculator.
- Every unobvious step in your computations must be explained. If you are genius enough to see the solution right away, you do not have to perform the whole derivation, but you have to convince me that the solution is correct.
- Every computation should be concluded by a clear answer.

Content

It may already not be enough to go through the problems in the homework. Check also everything we did during the exercises on the exercise sheets. Besides being able to do the computations, you should also know all the definitions and you should be able to describe all the algorithms we learned.

The structure of the exam will be as follows:

- 3 easier tasks per 8 points (such as questions on logic, determining gcd, remainders, prime decomposition, generators of a group, order of an element in a group, combinatorics, basic notions in graphs)
- 3 harder tasks per 14 points (Diophantine equation (or a problem related to that), determining properties of a relation, determining properties of an operation / algebraic structure, expressing a number in a given base, performing some graph algorithm)
- 1 describing some algorithm abstractly for 14 points. Here, you have to be as precise as possible! Even a person, who has never heard about this algorithm, should understand how it works and be able to perform it for any input. If you are struggling with explaining it in general, try at least on some example (but you won't get full points).

Sample exam

1. *(8 p.)* Define what a *tautological consequence* means. Prove the following tautological consequence.

$$(a \wedge (b \vee c)) \models (a \vee b)$$

2. *(8 p.)* Define the *order* of an element in a group. Determine the order of $[6]$ in $(\mathbb{Z}_{21}, +)$.

3. *(8 p.)* What is the remainder of $17^{135} + 18^{67} + 19^{256}$ when dividing by 17?

4. *(14 p.)*

a) Consider a triple of natural numbers $a, b, c \in \mathbb{N}$. How can you decide, whether the Diophantine equation $ax + by = c$ has a solution or not?
b) Find all pairs $x, y \in \mathbb{Z}$ that satisfy the equation $168x + 245y = 14$.

5. *(14 p.)* We define a relation R on $\mathbb{N}$ as follows: For any $k, l \in \mathbb{N}$, kRl if and only if $\gcd(k, l) = 2$.

a) Find all $n \in N$ such that $nR2$.
b) Define a *reflexive* relation. Decide, whether R is reflexive.
c) Define a *symmetric* relation. Decide, whether R is symmetric.
d) Define a *transitive* relation. Decide, whether R is transitive.

6. *(14 p.)*

a) Define *Eulerian graph* and *Eulerian circuit*.
b) Formulate a criterion how to decide, whether a graph is Eulerian or not.

Now, consider the graph $G = (V, E)$ with $V = \{1, 2, \ldots, 9\}$ and

$$E = \{\{1,2\},\{1,3\},\{2,3\},\{2,4\},\{2,5\},\{3,5\},\{3,7\},\{4,6\},\{4,8\},\{4,9\},\{5,6\},\{5,7\},\{6,8\},\{6,9\}\}$$

c) Use your criterion to decide, whether the graph is Eulerian.
d) If the graph is Eulerian, find the corresponding Eulerian circuit.

7. *(14 p.)* Define a *spanning tree*. Does every graph have a spanning tree? What is the necessary and sufficient condition to have one? Describe the Kruskal's algorithm.

Sample exam – solutions

1. *(8 p.)*

A propositional formula β is said to be a **tautological consequence** of a propositional formula α, denoted by $\alpha \models \beta$, if $\alpha \Rightarrow \beta$ is a tautology (it is true for every truth valuation).

We are going to prove the given one by filling the truth table a showing that $(a \wedge (b \vee c)) \Rightarrow (a \vee b)$ is indeed true for every truth valuation.

a	b	c	$a \wedge (b \vee c)$	$a \vee b$	$\Rightarrow$
F	F	F	F	F	T
F	F	T	F	F	T
F	T	F	F	T	T
F	T	T	F	T	T
T	F	F	F	T	T
T	F	T	T	T	T
T	T	F	T	T	T
T	T	T	T	T	T

2. *(8 p.)*

Let $(G, \cdot)$ be a group, $a \in G$. The smallest $j \in \mathbb{N}$ such that $a^j = e$ is called the **order** of a. If there is no such j, we say that the order is infinite.

To find the order of $[6]$ in $(Z_{21}, +)$, we just keep adding it until we get the neutral element $[0]$:

k	1	2	3	4	5	6	7
$k[6]$	[6]	[12]	[18]	[3]	[9]	[15]	[0]

So, the order is 7.

Alternatively, one can use Proposition 4.3.41 from the lecture which computes the order of $[k]$ in $(\mathbb{Z}_n, +)$ as $n/\gcd(n, k)$. In this case, we get $21/\gcd(21, 6) = 21/3 = 7$.

3. *(8 p.)*

All the computations will be modulo 17. We clearly have $17 \equiv 0$, so $17^{135} \equiv 0$. Also $18 \equiv 1$, so $18^{67} \equiv 1$. For the last term, we have two options. We can use Little Fermat's theorem, which implies that $19^{16} \equiv 1$ (as 17 is prime and $19 \perp 17$). Since $265 = 16 \cdot 16$, this means that $19^{256} \equiv 1$. Alternatively, we note that $19 \equiv 2$ and hence $19^4 \equiv 16 \equiv -1$, hence $19^8 \equiv 1$ and so $19^{256} \equiv 1$.

Together, this means that $17^{135} + 18^{67} + 19^{256} \equiv 0 + 1 + 1 \equiv 2$, so the remainder is 2.

4. *(14 p.)*

A solution of the Diophantine equation $ax + by = c$ exists if and only if $\gcd(a, b) \mid c$.

We find the solution of $168x + 245y = 14$ using the Euclid's algorithm:

$$\begin{aligned} 245 &= 1 \cdot 168 + 77 \\ 168 &= 2 \cdot 77 + 14 \\ 77 &= 5 \cdot 14 + 7 \\ 14 &= 2 \cdot 7 \end{aligned}$$

We see that the solution exists and we can find one by reversing the computation:

$$14 = 168 - 2 \cdot 77 = -2 \cdot 245 + 3 \cdot 168.$$

So, one solution is $x_0 = 3$, $y_0 = -2$. Finally, all solutions are then given by

$$x = 3 + \frac{245}{\gcd(168, 245)}k = 3 + 35k,$$
$$y = -2 - \frac{168}{\gcd(168, 245)}k = -2 - 24k, \qquad k \in \mathbb{Z}.$$

5. *(14 p.)*

a) $nR2 \quad \Leftrightarrow \quad \gcd(n, 2) = 2 \quad \Leftrightarrow \quad 2 \mid n$, so we get exactly all even numbers

b) A relation R on a set A is **reflexive** if $(\forall a \in A)(aRa)$.

Take any $k \in \mathbb{N}$. Then $\gcd(k, k) = k$. So, for instance, taking $k = 3$, we have $\gcd(3, 3) = 3 \neq 2$ and hence $3 \not R\, 3$, so the relation is not reflexive.

c) A relation R on a set A is **symmetric** if $(\forall a, b \in A)(aRb \Rightarrow bRa)$.

Since $\gcd(k, l) = \gcd(l, k)$, we clearly have $kRl \Leftrightarrow lRk$, so the relation is symmetric.

d) A relation R on a set A is **transitive** if $(\forall a, b, c \in A)((aRb \wedge bRc) \Rightarrow aRc)$

Take $a = c = 6$ and $b = 2$. Then $\gcd(a, b) = \gcd(b, c) = 2$, so aRb and bRc, but $\gcd(a, c) = 6$, so $a \not R\, c$. Hence, the relation is not transitive.

6. *(14 p.)*

a) Let $G = (V, E)$ be a graph. An **Eulerian circuit** is a circuit, where all edges are used exactly once. A graph is called **Eulerian** if it admits an Eulerian circuit.

b) A connected graph is Eulerian if and only if the degree of every its vertex is even.

c) We can just compute the degrees

v	1	2	3	4	5	6	7	8	9
$d(v)$	2	4	4	4	4	4	2	2	2

All are even, so the graph is Eulerian.

d) For instance, the following circuit is Eulerian:

$$1 - 2 - 3 - 5 - 6 - 8 - 4 - 6 - 9 - 4 - 2 - 5 - 7 - 3 - 1.$$

7. *(14 p.)* Let $G = (V, E)$ be a graph. A subgraph $G' = (V, E')$, $E' \subseteq E$ which is a tree is called a **spanning tree** of G. Such a spanning tree exists if and only if the graph is connected.

If we are given a cost function $c\colon E \to [0, +\infty)$ (i.e. a weighted graph), we may be interested in finding a *minimal spanning tree*, i.e. a spanning tree such that the it's cost $c(E') = \sum_{e \in E'} c(e)$ is minimal. Such a minimal spanning tree can be found by the Kruskal's algorithm that works as follows:

1. Sort the edges in E according to the cost c. That is, denote $E = \{e_1, \ldots, e_m\}$ such that

$$c(e_1) \leq c(e_2) \leq \cdots \leq c(e_m)$$

2. Put $E' := \emptyset$.
3. For every $i = 1, \ldots, m$, if the edge set $E' \cup \{e_i\}$ contains no cycle, put e_i to E'