1 Tutorial 1

1.1 Write down the truth tables of the following formulas. Decide whether they are tautologies:

a) $(x \Rightarrow y) \Rightarrow x$;

b) $\neg\neg\neg x \Leftrightarrow \neg x$;

c) $(x \vee y) \Leftrightarrow (y \Rightarrow x)$;

d) $((x \vee y) \vee z) \Leftrightarrow (x \vee (y \vee z))$;

e) $(x \Rightarrow (y \vee z)) \vee ((y \wedge z) \Rightarrow x)$.

Solution of e).

Denote $\alpha = (x \Rightarrow (y \vee z)) \vee ((y \wedge z) \Rightarrow x)$. Then the truth table is

x	y	z	$x \Rightarrow (y \vee z)$	$(y \wedge z) \Rightarrow x$	α
0	0	0	1	1	1
0	0	1	1	1	1
0	1	0	1	1	1
0	1	1	1	0	1
1	0	0	0	1	1
1	0	1	1	1	1
1	1	0	1	1	1
1	1	1	1	1	1

Since the column corresponding to α contains all 1's, α is a tautology.

1.2 For which truth valuations u is the formula

a) $(x \Rightarrow \neg x) \wedge (\neg x \Rightarrow x)$ true;

b) $x \Rightarrow (x \Rightarrow y)$ false;

c) $x \wedge (y \Rightarrow (z \vee x))$ true;

d) $(x \Rightarrow \neg x) \Leftrightarrow \neg x$ false;

e) $(x \vee \neg y) \Rightarrow (\neg x \wedge y)$ true;

f) $(((x \vee y) \wedge z) \wedge y) \vee x$ false?

Solution of f). We give two different solutions:

1. We can use the truth table for $\alpha = (((x \vee y) \wedge z) \wedge y) \vee x$

x	y	z	$x \vee y$	$(x \vee y) \wedge z$	$((x \vee y) \wedge z) \wedge y$	α
0	0	0	0	0	0	0
0	0	1	0	0	0	0
0	1	0	1	0	0	0
0	1	1	1	1	1	1
1	0	0	1	0	0	1
1	0	1	1	1	0	1
1	1	0	1	0	0	1
1	1	1	1	1	1	1

We can see that α is false for all valuations in which x is false and at least one of y and z is also false.

2. We can also proceed without the truth table. Since $\alpha = \beta \vee x$ (for $\beta = ((x \vee y) \wedge z) \wedge y$), α is true whenever x is true. So α could be false only for x false. Moreover, for α to be false, also β must be false. On the other hand, $\beta \nvDash y \wedge z$, therefore α is false for those truth valuations for which x and $z \wedge y$ are both false, which means that x is false and at least one of y and z is false as well.

1.3 Decide whether the following formulas are tautologies, contradictions, or satisfiable formulas that are not tautologies:

a) $(x \Rightarrow y) \Rightarrow (x \vee y)$;

b) $((x \Rightarrow y) \Rightarrow (\neg x \wedge y)) \vee \neg y$;

c) $((x \wedge y) \vee (\neg x \wedge \neg y)) \Leftrightarrow ((\neg x \vee \neg y) \wedge (x \vee y))$;

d) $(x \Rightarrow (x \Rightarrow y)) \Rightarrow y$;

e) $((x \Rightarrow z) \wedge (y \Rightarrow z)) \Rightarrow ((x \wedge y) \Rightarrow z)$;

f) $((x \Rightarrow z) \vee (y \Rightarrow z)) \Rightarrow (x \Rightarrow y)$.

Solution of f).

Denote $\alpha = ((x \Rightarrow z) \vee (y \Rightarrow z)) \Rightarrow (x \Rightarrow y)$. Again we show two different solutions.

1. We can use the truth table:

x	y	z	$x \Rightarrow z$	$y \Rightarrow z$	$(x \Rightarrow z) \vee (y \Rightarrow z)$	$x \Rightarrow y$	α
0	0	0	1	1	1	1	1
0	0	1	1	1	1	1	1
0	1	0	1	0	1	1	1
0	1	1	1	1	1	1	1
1	0	0	0	1	1	0	0
1	0	1	1	1	1	0	0
1	1	0	0	0	0	1	1
1	1	1	1	1	1	1	1

Hence α is a satisfiable formula but not a tautology.

2. We can also proceed as follows: The formula α is satisfiable, since for example if $u(x) = u(y) = 0$ (and $u(z)$ arbitrary), the formula α is true. Indeed, in this case $u(x \Rightarrow y) = 1$, therefore any formula of the form $\beta \Rightarrow (x \Rightarrow y)$ is true as well.

On the other hand, α is not a tautology, since for $u(x) = 1$, $u(y) = 0$ we have $u(x \Rightarrow y) = 0$ and at the same time $u(y \Rightarrow z) = 1$ regardless the value $u(z)$. Therefore, $u((x \Rightarrow z) \vee (y \Rightarrow)) = 1$ and α is false.

1.4 Show that the following semantical consequences are valid:

a) $\{\alpha \Rightarrow \beta, \beta \Rightarrow \gamma\} \models \alpha \Rightarrow \gamma$;

b) $\{\alpha \Rightarrow \beta, \neg\beta\} \models \neg\alpha$;

c) $\{\alpha \vee \beta, \alpha \Rightarrow \gamma, \beta \Rightarrow \gamma\} \models \gamma$;

d) $\{\alpha \Rightarrow \beta, \alpha \Rightarrow \neg\beta\} \models \neg\alpha$;

e) $\{(\alpha \wedge \beta) \Rightarrow \gamma, (\alpha \wedge \neg\beta) \Rightarrow \gamma\} \models \alpha \Rightarrow \gamma$.

Solution of c).

Denote $S = \{\alpha \vee \beta, \alpha \Rightarrow \gamma, \beta \Rightarrow \gamma\}$. We show two different solutions.

1. We will use the truth table.

α	β	γ	$\alpha \vee \beta$	$\alpha \Rightarrow \gamma$	$\beta \Rightarrow \gamma$	S	γ
0	0	0	0	1	1	0	0
0	0	1	0	1	1	0	1
0	1	0	1	1	0	0	0
0	1	1	1	1	1	1	1
1	0	0	1	0	1	0	0
1	0	1	1	1	1	1	1
1	1	0	1	0	0	0	0
1	1	1	1	1	1	1	1

We can see from the truth table that whenever S is true in u formula γ is true as well. Therefore, γ is a consequence of S.

2. We show that if in a truth valuation u the formula γ is false, then at least one of the formulas from S is false as well.

Assume that $u(\gamma) = 0$. Then either $u(\alpha) = 1$ but then $u(\alpha \Rightarrow \gamma) = 0$ (and $u(S) = 0$); or $u(\alpha) = 0$. Similarly, $u(\beta) = 1$ yields $u(\beta \Rightarrow \gamma) = 0$ (and $u(S) = 0$); or $u(\beta) = 0$. But if $u(\alpha) = 0 = u(\beta)$ then $u(\alpha \vee \beta) = 0$ (and again $u(S) = 0$. Therefore, there is no u for which $u(S) = 1$ and $u(\gamma) = 0$, which proves that $S \models \gamma$.

1.5 Write down values of the boolean function g given bellow and try to simplify it:

a) $g(x, y, z) = (x + \overline{y} + z)\,(\overline{x} + \overline{y} + \overline{z})\,(\overline{x} + y + \overline{z})$;

b) $g(x, y, z) = (x + y + z)\,(\overline{x} + \overline{y} + \overline{z})\,(\overline{x} + \overline{y} + z)\,(x + \overline{y} + \overline{z})$.

Solution of b).

We will display the values of $g(x, y, z)$ in the following table. The eight rows express the eight combinations of 0 and 1 we can substitute into g. For example,

$$g(0, 0, 0) = (0 + 0 + 0)\,(1 + 1 + 1)\,(1 + 1 + 0)\,(0 + 1 + 1) = 0 \cdot 1 \cdot 1 \cdot 1 = 0.$$

Similarly, $g(0, 0, 1)$, etc. We get:

x	y	z	$g(x, y, z)$
0	0	0	0
0	0	1	1
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	1
1	1	0	0
1	1	1	0

To simplify the boolean function $g(x, y, z)$ we will use the the distributivity law:

$$(\overline{x} + \overline{y} + \overline{z})\,(\overline{x} + \overline{y} + z) = (\overline{x} + \overline{y})\,(z + \overline{z}) = (\overline{x} + \overline{y}) \cdot 1 = (\overline{x} + \overline{y}).$$

and

$$(\overline{x} + \overline{y} + \overline{z})\,(x + \overline{y} + \overline{z}) = (\overline{x} + x)\,(\overline{y} + \overline{z}) = 1 \cdot (\overline{y} + \overline{z}) = (\overline{y} + \overline{z}).$$

Hence

$$g(x, y, z) = (x + y + z)\,(\overline{x} + \overline{y})\,(\overline{y} + \overline{z}).$$

Answers

1.1 a) not a tautology, b) a tautology, c) not a tautology, d) a tautology, e) a tautology.

1.2 a) In no truth valuation. b) For the truth value for which $u(x) = 1$, $u(y) = 0$. c) For all truth valuations for which we have $u(x) = 1$. d) In no truth valuation. e) For truth valuation with $u(x) = 0$ and $u(y) = 1$. f) For all truth valuations for which the logical variable x is false and at least one from logical variables y, z is also false. It means $u(x) = 0$ and at the same time $u(y) = 0$ or $u(z) = 0$.

1.3 a) A satisfiable formula which is not a tautology. b) A satisfiable formula which is not a tautology. c) A contradiction. d) A satisfiable formula which is not a tautology. e) A tautology. f) A satisfiable formula which is not a tautology.

1.5 a) $g(x, y, z) = x\overline{z} + \overline{x}y + \overline{y}\overline{z} = (\overline{x} + \overline{z})\,(x + \overline{y} + z)$.

2 Tutorial 2

2.1 Write formulas of predicate logic corresponding to the following sentences. Use the predicate symbols mentioned in the text.

a) Somebody has a musical ear (E) and somebody does not.

b) Some children (C) do not like chocolate (H).

c) Not every talented painter (P) exhibits his/her pictures in the National Gallery (G).

d) Only students (S) can buy cold suppers (C).

e) Not every person (P) who has expensive skis (E), is a bad skier (B).

2.2 Find predicate symbols, constant symbols, and functional symbols which are needed to formalize the following statements as formulas of predicate logic.

a) The square of an odd number is always odd.

b) If a natural number is divisible by six then it is also divisible by three.

c) There are numbers a, b, and c such that the sum of the squares of a and b equals the square of c.

d) Every tetragon whose diagonals are equal is a rhombus.

2.3 Given predicate symbols P, Q, functional symbols f, s, and constant symbols a, and b. Moreover, Q and f are binary, and P and s unary. Decide which of the following strings are well formed formulas of predicate logic. If a string is a formula draw its derivation tree.

a) $Q(f(a), s(b))$;

b) $P(f(x, s(x)))$;

c) $\forall x\,(Q(f(x, a), b) \Rightarrow P(f(a, b)))$;

d) $(\forall x\,P(f(x, b)) \Rightarrow (\exists y\,Q(f(y), P(y)))$;

e) $(P(x) \wedge Q(f(x, y)) \Rightarrow (\exists y\,(P(y) \vee P(f(y)))$;

f) $\exists x\,(P(Q(x, y)) \Rightarrow Q(a, b))$;

g) $\forall x(P(x) \Rightarrow (\exists y\,Q(x, y)))$.

2.4 A predicate logic language has the following special symbols: predicate symbols P, Q, and functional symbols f, g. All symbols are unary.

Given an interpretation $\langle U, [\![-]\!]\rangle$, where U is the set of all people,
f is interpreted as a father, i.e. $[\![f]\!]$ assigns to a person x his/her father,
g is interpreted as a mother, i.e. $[\![g]\!]$ assigns to a person x his/her mother,
P is interpreted as the property "to play piano", and Q is interpreted as the property "to play guitar".

Write the sentences that correspond to the following sentences in the given interpretation:

a) $\forall x\,(P(f(x)) \vee Q(g(x)))$;

b) $\exists x\,(P(g(x)) \wedge Q(f(x)))$;

c) $\forall x\,((P(f(x)) \vee Q(g(x))) \Rightarrow (P(x) \vee Q(x)))$;

d) $\exists x\,(P(g(f(x)))$;

e) $\exists y\,(P(y) \wedge \neg Q(f(g(y))))$;

2.5 For each of the following sentences, decide whether it is a tautology, a contradiction, or a satisfiable sentence which is not a tautology. (P is a unary, and Q is a binary predicate symbol.)

a) $(\exists x\, P(x)) \vee (\exists x\, \neg P(x))$;

b) $\forall x\, (P(x) \vee \neg P(x))$;

c) $(\exists x\, P(x)) \Rightarrow (\forall x\, P(x))$;

d) $(\forall x\, P(x)) \wedge (\exists x\, \neg P(x))$;

e) $\forall x\, [\exists y\, Q(x,y) \vee \forall z\, \neg Q(x,z)]$.

2.6 Decide whether the following sets of sentences are satisfiable or not. State the reasons. (P and R are unary predicate symbols, Q is a binary predicate symbol.)

a) $S = \{\forall x\, \exists y\, Q(x,y), \forall x\, \neg Q(x,x)\}$;

b) $S = \{\exists x\, \forall y\, Q(x,y), \forall x\, \neg Q(x,x)\}$;

c) $S = \{\forall x\, (P(x) \vee R(x)), \neg \exists x\, R(x), \neg P(a)\}$.

2.7 For the sentence φ find a sentence ψ which is tautologically equivalent to $\neg\varphi$ and such that ψ has the negations only before atomic formulas. (P is a unary predicate symbol, R is a binary predicate symbol, and a is a constant symbol.)

a) $\forall x\, [P(x) \Rightarrow (\exists y\, (P(y) \wedge R(x,y)))]$;

b) $P(a) \vee [\exists z\, (P(z) \wedge \forall y\, (R(y,z) \Rightarrow \neg P(y)))]$.

2.8 Show that the following inferences are valid.

1. $\{P(a), \forall x\, (\neg P(x) \vee Q(x))\} \models Q(a)$.
2. $\{\forall x\, (P(x) \Rightarrow Q(x)), \exists x\, P(x)\} \models \exists x\, Q(x)$.
3. $\{\exists x\, \neg Q(x), \{\forall x\, (P(x) \Rightarrow Q(x))\} \models \exists x\, \neg P(x)$.

2.9 Given a formula α of predicate logic. Write down the formula β tautologically equivalent to $\neg\alpha$ which has negation in front of atomic formulas only.

a) $\alpha = R(a) \wedge \forall x\, (Q(x,a) \Rightarrow \exists y\, (R(y) \wedge Q(x,y)))$.

b) $\alpha = \forall x\, (P(x) \Rightarrow \exists y\, (Q(x,y) \wedge P(y)))$.

Solution of a). We have

$$\neg\alpha = \neg(R(a) \wedge \forall x\, (Q(x,a) \Rightarrow \exists y\, (R(y) \wedge Q(x,y)))).$$

Since the last logical connective is $\wedge$, we have

$$\neg\alpha \leftrightharpoons \neg R(a) \vee \neg(\forall x\, (Q(x,a) \Rightarrow \exists y\, (R(y) \wedge Q(x,y))))).$$

Moreover,

$$\neg(\forall x\, (Q(x,a) \Rightarrow \exists y\, (R(y) \wedge Q(x,y)))) \leftrightharpoons \exists x\, \neg(Q(x,a) \Rightarrow \exists y\, (R(y) \wedge Q(x,y))),$$

and

$$\neg(Q(x,a) \Rightarrow \exists y\, (R(y) \wedge Q(x,y)) \leftrightharpoons Q(x,a) \wedge \neg(\exists y\, (R(y) \wedge Q(x,y)))).$$

Finally,

$$\neg\exists y\,(R(y) \wedge Q(x,y)) \;\models\!\!\models\; \forall y\,(\neg R(y) \vee \neg Q(x,y)).$$

Hence

$$\beta = \neg R(a) \vee \exists x\,(Q(x,a) \wedge \forall y\,(\neg R(y) \vee \neg Q(x,y))).$$

Answers

2.1 a) $(\exists x\,E(x)) \wedge (\exists x\,\neg E(x))$;
b) $\exists x\,(C(x) \wedge \neg H(x))$;
c) $\neg(\forall x\,(P(x) \Rightarrow G(x)))$;
d) $\forall x\,(C(x) \Rightarrow S(x))$;
e) $\neg[\forall x\,((P(x) \wedge E(x)) \Rightarrow B(x))]$.

2.2 The formulas can be formed in different ways. We give one of them.

a) Objects are natural numbers. The predicate symbol O represents the property "to be an odd number", the functional symbol f corresponds to the function which assigns to a number n its square n^2. Then the formula has the following form:
$\forall x\,(O(x) \Rightarrow O(f(x)))$.

b) Objects are natural numbers. The predicate symbol Q represents the relation of divisibility on $\mathbb{N}$, the constant symbol a is 6, and the constant symbol b is 3. The formula has the following form:
$\forall x\,(Q(a,x) \Rightarrow Q(b,x))$.

c) Objects are natural numbers. The predicate symbol $=$ represents a well known equality, the functional symbol $+$ is binary and represents addition of natural numbers, the functional symbol f is unary and it assigns to every natural number its square. The formula has the following form:
$\exists x\,\exists y\,\exists z\,(f(x) + f(y) = f(z))$.

2.3 a) It is not a formula, since $f(a)$ is not a term. b) A formula. c) A formula. d) It is not a formula, since $P(y)$ is not a term. e) It is not a formula, since $f(y)$ is not a term. f) It is not a formula, since $Q(x,y)$ is not a term. g) A formula.

2.4 a) For all people it holds that their father plays piano or their mother plays guitar. b) There is a person whose mother plays piano and whose father plays guitar. c) If a person's father plays piano or his/her mother plays guitar then the person himself/herself plays piano or guitar. d) Somebody has a grandmother from the father side who plays piano. e) Somebody plays piano even though his/her grandfather from the mother side does not play guitar.

2.5 a) A tautology. b) A tautology.
c) A satisfiable sentence which is not a tautology. Verification: The sentence $(\exists x\,P(x)) \Rightarrow (\forall x\,P(x))$ is true whenever the sentence $\exists x\,P(x)$ is false. Consider the following interpretation: U is the set of real numbers, P is interpreted as the property "to be a square root of -1". Since no real number has the property $I(P)$, our sentence is true in $\langle U, [\![-]\!]\rangle$.
On the other hand, consider the interpretation: U' is the set of natural numbers, P is interpreted as the property "to be even". Then the sentence $\exists x\,P(x)$ is true in U', I', because there exists an even number. On the other hand, the sentence $\forall x\,P(x)$ is, of course, false, since it is not the case that all natural numbers are even. Hence, we have shown that the sentence $(\exists x\,P(x)) \Rightarrow (\forall x\,P(x))$ is false in $\langle U', [\![-]\!]\rangle$.
d) A contradiction. e) A tautology.

2.6 a) S is satisfiable. Its model is, for instance, the following interpretation: $U = \mathbb{N}$, $[\![Q]\!]$ is the relation $<$ on the set $\mathbb{N}$, i.e. $[\![Q]\!] = \{(m, n) \mid m < n\}$. Then for every natural number n there exists a bigger number (e.g. $n + 1$), and no natural number is bigger than itself.

b) S is unsatisfiable. Let us read the first sentence: "There exists an element, say d, such that for every element y the pair (d, y) has the property Q." If we substitute the element d for y, the pair (d, d) also has the property Q. Hence the second sentence cannot be true. Indeed, it says: "For no element x the pair (x, x) has the property Q."

Formally: Take any interpretation $\langle U, [\![-]\!]\rangle$, in which the sentence $\exists x\, \forall y\, Q(x, y)$ is true. Then there exists an element $d \in U$ such that for every element $d' \in U$ the pair (d, d') belongs to $[\![Q]\!]$. Therefore also $(d, d) \in [\![Q]\!]$. This means that the sentence $\forall x\, \neg Q(x, x)$ is false in $\langle U, [\![-]\!]\rangle$.

c) S is unsatisfiable. Let us read the first and the third sentences: "Every element has the property P or the property R." "The element a does not have the property P." If both the sentences are true in an interpretation, then the element a has the property R. It means that the second sentence: "No element has the property R." is false. Formally: Take any interpretation $\langle U, [\![-]\!]\rangle$, in which the first and the third sentences are true. Then there is an element $d \in U$ $(d = [\![a]\!])$ such that $d \notin [\![P]\!]$. Since the $\forall x\, (P(x) \vee R(x))$ is true in $\langle U, [\![-]\!]\rangle$, the sentence $P(a) \vee R(a)$ is true in $\langle U, [\![-]\!]\rangle$. It means that the sentence $R(a)$ is true. Thus $d = [\![a]\!] \in [\![Q]\!]$. Therefore the sentence $\forall x\, \neg R(x)$ is false in $\langle U, [\![-]\!]\rangle$.

2.7 a) $\exists x\, [P(x) \wedge \forall y\, (\neg P(y) \vee \neg R(x, y))]$.

b) $\neg P(a) \wedge \forall z\, (\neg P(z) \vee \exists y\, (R(y, z) \wedge P(y)))$.

2.8 a) Take any interpretation $\langle U, [\![-]\!]\rangle$ in which both sentences $P(a)$ and $\forall x\, (\neg P(x) \vee Q(x))$ are true. Since the element $d \in U$ corresponding to a has property corresponding to P, d must have the property corresponding to Q (otherwise the formula $\forall x\, (\neg P(x) \vee Q(x)$ will be false). This means that $Q(a)$ is true in $\langle U, [\![-]\!]\rangle$.

b) ake any interpretation $\langle U, [\![-]\!]\rangle$ in which both sentences $\forall x\, (P(x) \Rightarrow Q(x))$ and $\exists x\, P(x)$ are true. Since $\exists x\, P(x)$ is true, there is $d \in U$ which has the property corresponding to P. Substitute d for x. Then from the second sentence we get that d must also have the property corresponding to Q. Hence $\exists x\, Q(x)$ is true in $\langle U, [\![-]\!]\rangle$.

c) It is a special case of b), since $\forall x\, (P(x) \Rightarrow Q(x))$ is tautologically equivalent to $\forall x\, (\neg Q(x) \Rightarrow \neg P(x))$.

2.9 b) $\beta = \exists x\, (P(x) \wedge \forall y\, (\neg Q(x, y) \vee \neg P(y)))$.

3 Tutorial 3

3.1 Which conditions must be satisfied by sets A, B, C to guarantee that:

a) $(A \setminus C) \setminus B = A \setminus (C \setminus B)$;

b) $A \cap (B \cup C) = (A \cap B) \cup C$;

c) $A \cup (B \oplus C) = (A \cup B) \oplus (A \cup C)$;

d) $A \setminus (B \cup C) = (A \setminus B) \setminus C$;

e) $(A \cap B) \setminus C = A \cap (B \setminus C)$;

f) $A \cap (B \setminus C) = (A \setminus C) \cap B$;

g) $A \cup (B \setminus C) = (A \cup B) \setminus (A \cup C)$.

Solution of b). Take any $x \in A \cap (B \cup C)$. Then $x \in A$ and $x \in B \cup C$, which means $x \in A$ and ($x \in B$ or $x \in C$). From the propositional logic we know that it is equivalent to ($x \in A$ and $x \in B$) or ($x \in A$ and $x \in C$).

On the other hand, $x \in (A \cap B) \cup C$ means that ($x \in A$ and $x \in B$) or $x \in C$. Hence for the two conditions to be the same we must have $x \in A$ and $x \in C$ is the same as $x \in C$. And this is just when all $x \in C$ belong to A as well, i.e. $C \subseteq A$.

3.2 Decide whether or not the following assertions hold; give arguments for your answers.

a) $A \times B = \emptyset$ if and only if $A = \emptyset$ or $B = \emptyset$.

b) For all sets A, B we have $A \times B = B \times A$.

c) For all sets A, B, C the following holds: If $B \subseteq C$, then $A \times B \subseteq A \times C$.

d) If $A \times B \subseteq A \times C$, then $B \subseteq C$.

e) $A \times (B \cup C) = (A \times B) \cup (A \times C)$.

f) $A \times (B \cap C) = (A \times B) \cap (A \times C)$.

g) $(B \oplus C) \times A = (B \times A) \oplus (C \times A)$.

h) If $A \oplus B = A \oplus C$, then $B = C$.

i) $A \setminus (B \oplus C) = (A \setminus B) \oplus (A \setminus C)$.

Solution of e). First we show that $A \times (B \cup C) \subseteq (A \times B) \cup (A \times C)$.

Consider any pair $(x, y) \in A \times (B \cup C)$. Then $x \in A$, and y is at least in of the sets B, C. Hence, $x \in A$ and $y \in B$, or $x \in A$ and $y \in C$. It means that $(x, y) \in A \times B$, or $(x, y) \in A \times C$.

Now we show that $(A \times B) \cup (A \times C) \subseteq A \times (B \cup C)$.
Consider any $(x, y) \in (A \times B) \cup (A \times C)$. Then $x \in A$ and $y \in B$, or $x \in A$ and $y \in C$. In both cases $x \in A$, and y is in at least one of B and C. Hence, $(x, y) \in A \times (B \cup C)$.

Therefore, $A \times (B \cup C) = (A \times B) \cup (A \times C)$ holds.

3.3 List all the subsets of the set $\{1, 2, 3, 4\}$. How many are there?

Solution. $\emptyset$, $\{1\}$, $\{2\}$, $\{3\}$, $\{4\}$, $\{1, 2\}$, $\{1, 3\}$, $\{1, 4\}$, $\{2, 3\}$, $\{2, 4\}$, $\{3, 4\}$, $\{1, 2, 3\}$, $\{1, 2, 4\}$, $\{1, 3, 4\}$, $\{2, 3, 4\}$, $\{1, 2, 3, 4\}$. There are $2^4 = 16$ subsets.

3.4 There are 200 students in a school, 140 of them can speak French, 80 students can speak German, and 20 students do not know either of these languages. How many students speak both languages?

Solution. Denote by F the set of all students who speak French, and by G the set of all students who speak German. The union $F \cup G$ has $200 - 20 = 180$ students. Moreover, if we add the number of students in F and the number of students in G we the number of students in $F \cup G$ plus the number of students in $F \cap G$. Hence, in $F \cap G$ there are $140 + 80 - 180 = 40$ students.

3.5 Let $A = \{0, 1, 2\}$ and $B = \{a, b\}$. List all mappings from A into B. How many maps are there? Which of them are injective? Which of them are surjective?

Solution. There are $2^3 = 8$ mappings; indeed, 0 can be mapped to either of a and b, the same hold for 1 and 2 as well.

None is injective; there exists no injective mapping from A to B whenever both are finite and A has more elements than B (see Pigeonhole Principle).

There are only two mappings that are not surjective; indeed, they are f and g, where $f(0) = f(1) = f(2) = a$ and $g(0) = g(1) = g(2) = b$. So, there are $8 - 2 = 6$ surjective mapping from A to B.

3.6 Find an example of a mapping $f : \mathbb{N} \longrightarrow \mathbb{N}$ such that

a) f is injective but not surjective,
b) f is surjective but not injective,
c) f is injective and surjective,
d) f is neither injective nor surjective.

3.7 Show that the rule

$$(m, n) \mapsto 2^m(2n + 1) - 1 \quad (m, n \in \mathbb{N})$$

defines an injective mapping of the set $\mathbb{N} \times \mathbb{N}$ onto $\mathbb{N}$.

3.8 Show that the set of all binary words is countable. (A binary word is a finite sequence of 0's and 1's.)

3.9

a) Show that any two non-empty open intervals (a, b) and (c, d) of real numbers have the same cardinality.
b) Show that the set $\mathbb{R}$ and the set of all positive real numbers $(0, \infty)$ have the same cardinality.

Answers

3.1 a) $A \cap B = \emptyset$; b) $C \subseteq A$; c) $A = \emptyset$; d) holds for arbitrary sets A, B, C; e) holds for arbitrary sets A, B, C; f) holds for arbitrary sets A, B, C; g) $A = \emptyset$.

3.2 a) True. b) False, for instance, $\{1\} \times \{2\} = \{(1, 2)\} \neq \{(2, 1)\} = \{2\} \times \{1\}$. c) True. d) False; for instance, $\emptyset \times \{2\} = \emptyset \subseteq \emptyset = \emptyset \times \{3\}$ and $\{2\} \not\subseteq \{3\}$. e) True. f) True.
g) True. h) True. i) False; for example, if $A = \{1, 2\}$, $B = \{2, 3\}$, $C = \{3, 4\}$ then $A \setminus (B \oplus C) = \{1\}$, $(A \setminus B) \oplus (A \setminus C) = \{2\}$.

3.6 There are many functions for each task, we give always one possible solution.

a) For example, $f(n) = n + 1$. Indeed, there is no natural number i for which $i + 1 = 0$.

b) For example, $f(0) = 0$ and $f(n) = n - 1$ for all $n \geq 1$. ($f(0) = f(1)$, so f is not injective.)

c) For example, $f(n) = n+1$ for n even, and $f(n) = n-1$ for n odd. Indeed, the image of an even number is always odd and the image of an odd number is always even. Moreover, no distinct even numbers are mapped on the same odd number, as well no distinct odd numbers are mapped on the same even number. Hence f is injective. Take any $m \in \mathbb{N}$. Then m is either odd or even. If m is odd then $f(m-1) = m$, if m is even then $f(m+1) = m$. This shows that f is surjective.

d) For example, $f(n) = (n-3)^2$ is neither injective nor surjective. Indeed, $f(1) = 4 = f(5)$, hence f is not injective. Moreover, there is no $n \in \mathbb{N}$ for which $f(n) = (n-3)^2 = 2$. Hence, f is not surjective.

3.9 a) If we have two non-empty intervals of real numbers (a, b) and (c, d) then the linear function $f(x) = \frac{d-c}{b-a}(x - a) + c$ maps the interval (a, b) bijectively to (c, d).

b) Consider the function $f(x) = 2^x$. It is an injective function (increasing) and it maps the set of all real numbers $\mathbb{R}$ onto $(0, \infty)$.

4 Tutorial 4

4.1 Write the following relations on a set A as sets of ordered pairs:

a) A is the set of all subsets of the set $\{1,2\}$, relation R is "to be a proper subset". This means that for $X, Y \in A$ we have $X\,R\,Y$ if and only if $X \subseteq Y$ and $X \neq Y$.

b) $A = \{2,4,5,8,45,60\}$, R is the relation of divisibility; i.e. $m\,R\,n$ if and only if m divides n.

4.2 A relation R on a closed interval $A = [0,4]$ is given by:

$$x\,R\,y \quad \text{if and only if} \quad x^2 + y^2 + 7 \leq 4x + 4y.$$

Decide a) whether $2(\,R \circ R\,)2$ and b) whether $0\ (R^{-1} \circ R)\ 3$.

Solution of a). $2(\,R \circ R\,)2$ means that there exists $z \in [0,4]$ for which

$$2\,R\,z \quad \text{and} \quad z\,R\,2.$$

From the definition of R we know that $z\,R\,2$ holds if and only if $z^2 + 4 + 7 \leq 4z + 8$. And this reduces to the following quadratic equation $z^2 - 4z + 3 \leq 0$. Similarly, $2\,R\,z$ yields to $4 + z^2 + 7 \leq 8 + 4z$ which represents the same quadratic equation.

Since $z^2 - 4z + 3 = (z-3)\cdot(z-1)$, we get that $z^2 - 4z + 7 \leq 0$ if and only if $z \in [1,3]$. Therefore, $2\,R\,\frac{3}{2}$ holds. Hence, $2(\,R \circ R\,)2$ holds.

4.3 A relation R on a closed interval $A = [0,1]$ is given by: $x\,R\,y$ if and only if $y = 2|x - \frac{1}{2}|$. Sketch in a plane (as a set of ordered pairs) the relations R, R^{-1} and $R \circ R^{-1}$.

4.4 Give the properties of the following relations on the set of all natural numbers $\mathbb{N}$:

a) $m\,R\,n$ if and only if m divides n;

b) $m\,R\,n$ if and only if $m + n \geq 50$;

c) $m\,R\,n$ if and only if $m + n$ is even;

d) $m\,R\,n$ if and only if $m \cdot n$ is even;

e) $m\,R\,n$ if and only if $m = n^k$ for some $k \in \mathbb{N}$;

f) $m\,R\,n$ if and only if $m + n$ is a multiple of 3;

g) $m\,R\,n$ if and only if $m > n$.

Solution of d). R is not reflexive. Indeed, R is reflexive if for every natural number n we have $n\,R\,n$. This means that $n \cdot n$ is an even number. This is not true, because for example $3 \cdot 3 = 9$ which is an odd number.

R is symmetric. Indeed. assume that $n\,R\,m$ for some $n, m \in \mathbb{N}$. Then $n \cdot m$ is an even number. Because $m \cdot n = n \cdot m$ we also have $m\,R\,n$.

R is not antisymmetric; indeed, we have $2\,R\,3$ and $3\,R\,2$, but $2 \neq 3$.

R is not transitive. Indeed, for example $3\,R\,2$ (because $3 \cdot 2 = 6$ which is an even number), and so is $2\,R\,3$ but $3\,R\,3$ does not hold (because $3 \cdot 3 = 9$ is an odd number).

4.5 In the following examples S is a relation on a set A and x, y are elements of set A. Decide whether S is reflexive, symmetric, antisymmetric, transitive. Is it an equivalence, an order relation?

a) A is the set of all complex numbers, $x\,S\,y$ if and only if $|x| = |y|$.

b) A is the set of all complex numbers, $x\,S\,y$ if and only if $|x| < |y|$.

c) A is the set of all real numbers, $x\,S\,y$ if and only if $x - y$ is a rational number.

d) A is the set of all triangles of a given plane, two triangles are related in S if and only if they are congruent.

e) A is the set of all triangles of a given plane, two triangles are related in S if and only if they are similar.

f) A is the set of all subsets of a set B, two subsets X, Y of the set B are related in S if and only if they have the same cardinality; i.e., if and only if there exists an injective mapping of X onto Y.

Solution of a). S is reflexive; indeed, for every complex number z we have $|z| = |z|$, so $z\,S\,z$.

S is symmetric; indeed, if for two complex numbers x and y we have $|x| = |y|$, then so $|y| = |x|$, hence $y\,S\,x$.

S is not antisymmetric; indeed, we have $|1| = |i|$ (i is the imaginary unit), hence $1\,S\,i$ and $i\,S\,1$ but $1 \neq i$.

S is transitive; indeed, if for three complex numbers x, y, z we have $|x| = |y|$ and $|y| = |z|$, then $|x| = |z|$.

Therefore, S is an equivalence relation on the set of all complex numbers.

4.6 Given two relations R and S from a set A into a set B. Decide whether the following is true:

a) $(R \cup S)^{-1} = R^{-1} \cup S^{-1}$;

b) $(R \cap S)^{-1} = R^{-1} \cap S^{-1}$.

Solution of a) To show the statement, it is convenient to look at relations as a set of ordered pairs. We know that $R, S \subseteq A \times B$ and $R^{-1}, S^{-1} \subseteq B \times A$. Moreover, $(a, b) \in R$ if and only if $(b, a) \in R^{-1}$.

Hence we have, $(b, a) \in R^{-1} \cup S^{-1}$ if and only if $(b, a) \in R^{-1}$ or $(b, a) \in S^{-1}$ and it is if and only if $(a, b) \in R$ or $(a, b) \in S$. It means that $(a, b) \in R \cup S$ hence $(b, a) \in (R \cup S)^{-1}$.

Therefore, the equality holds.

4.7 Given two relations R and S on a set A. Decide whether it is true:

a) If R and S are reflexive, then so is $R \circ S$.

b) If R and S are symmetric, then so is $R \circ S$.

c) If R and S are antisymmetric, then so is $R \circ S$.

d) If R and S are transitive, then so is $R \circ S$.

Solution of b).

It does not hold. By the symmetry of R and S we can only say: If $x\,R\circ S\,y$, then $y\,S\circ R\,x$. Let us give an example of two relations R and S on the set of all real numbers $\mathbb{R}$, which are symmetric and such that $R\circ S$ is not symmetric. Let $x\,R\,y$ if and only if $|x-y|=1$, and $x\,S\,y$ if and only if $x^2+y^2=2$. Then $1\,R\,0$ and $0\,S\,\sqrt{2}$; hence $0\,R\circ S\,\sqrt{2}$. There exist only two real numbers z for which $\sqrt{2}\,R\,z$: $z_1=1+\sqrt{2}$ and $z_2=-1+\sqrt{2}$. For none of them do we have $z_i\,S\,1$, since $z_i^2+1\neq 2$. Therefore the relation $R\circ S$ is not symmetric.

Answers

4.1

a) $R=\{(\emptyset,\{1\}),(\emptyset,\{2\}),(\emptyset,\{1,2\}),(\{1\},\{1,2\}),(\{2\},\{1,2\})\}$.

b) $R=\{(2,2),(2,4),(2,8),(2,60),(4,4),(4,8),(4,60),(5,5),(5,45),(5,60),(8,8),(45,45),(60,60)\}$.

4.2 b) $0\ (R^{-1}\circ R)\ 3$ does not hold.

4.3

- The set of ordered pairs (x,y) for which $x\,R\,y$ is the graph of the function $y=2|x-\frac{1}{2}|$ for $x\in[0,1]$.
- The set of ordered pairs (x,y) for which $x\,R^{-1}\,y$ consists of the graphs of $y=\frac{1}{2}(1-x)$ and of $y=\frac{1}{2}(1+x)$ both for $x\in[0,1]$.
- The set of ordered pairs (x,y) for which $x\,R\circ R^{-1}\,y$ consists of the graphs of $y=x$ and of $y=1-x$ both for $x\in[0,1]$.

4.4

a) It is reflexive, antisymmetric, and transitive; i.e., a partial order.

b) It is only symmetric.

c) It is reflexive, symmetric, and transitive; i.e., an equivalence relation.

d) It is only symmetric.

e) It is reflexive, antisymmetric, and transitive; i.e., a partial order.

f) It is only symmetric.

g) It is only antisymmetric and transitive.

4.5

b) Antisymmetric, transitive; it is neither an equivalence nor a partial order.

c) Reflexive, symmetric, and transitive; an equivalence relation.

d) Reflexive, symmetric, and transitive; an equivalence relation.

e) Reflexive, symmetric, and transitive; an equivalence relation.

f) Reflexive, symmetric, and transitive; an equivalence relation.

4.6 b) It holds.

4.7

a) It holds.

c) It does not hold. For instance, consider the following antisymmetric relations on the set $\mathbb{N}$ of all natural numbers: $x\,R\,y$ if and only if $x \leq y$, and $x\,S\,y$ if and only if x divides y. Then $2\,R \circ S\,0$, since $2 \leq 3$ and 3 divides 0. Further, $0\,R \circ S\,2$, since $0 \leq 1$ and 1 is a divisor of 2. On the other hand, $0 \neq 2$.

d) It does not hold. A simple counter-example is the following: $A = \{1, 2, 3, 4, 5\}$, $R = \{(1, 2), (3, 4)\}$ (i.e. there is only $1\,R\,2$ and $3\,R\,4$), $S = \{(2, 3), (4, 5)\}$. Then $1\,R \circ S\,3$ and $3\,R \circ S\,5$, although it is not true $1\,R \circ S\,5$. We get a similar result if we consider relations R and S on the set of complex numbers, where $x\,R\,y$ if and only if $x - y$ is a rational number, $x\,S\,y$ if and only if $|x| = |y|$.

5 Tutorial 5

5.1 Using the Euclid's Algorithm find the greatest common divisor of 346 and 36.

Solution. 1. We set $u := 346$, $t := 36$.

2. We divide u by t:

$$346 = 9 \cdot 36 + 22,$$

and we set $u := 36$, $t := 22$.

3. Since $t \neq 0$, we divide u by t:

$$36 = 1 \cdot 22 + 14,$$

and we set $u := 22$, $t := 14$.

4. Since $t \neq 0$, we divide u by t:

$$22 = 1 \cdot 14 + 8,$$

and we set $u := 14$, $t := 8$.

5. Since $t \neq 0$, we divide u by t:

$$14 = 1 \cdot 8 + 6.$$

and we set $u := 8$, $t := 6$.

6. Since $t \neq 0$, we divide u by t:

$$8 = 1 \cdot 6 + 2,$$

and we set $u := 6$, $t := 2$.

7. Since $t \neq 0$, we divide u by t:

$$6 = 3 \cdot 2 + 0,$$

and we set $u := 2$, $t := 0$.

8. Since $t = 0$, we return $c := t = 2$.

The greatest common divisor $\gcd(346, 36) = 2$.

5.2 Find all the solutions of the following Diophantic equation

$$319\,x + 473\,y = 0.$$

Solution. First, we use the Euclid's algorithm to find $\gcd(319, 473)$. We proceed faster than in the first exercise.

$$\begin{array}{rcrcr} 319 & = & 0 \cdot 473 & + & 319 \\ 473 & = & 1 \cdot 319 & + & 154 \\ 319 & = & 2 \cdot 154 & + & 11 \\ 154 & = & 14 \cdot 11 & + & 0 \end{array}$$

We have obtained $\gcd(319, 473) = 11$.

We divide the equation by $\gcd(319, 473) = 11$ and we get

$$29\,x + 43\,y = 0.$$

This equation has the following general solution: $x = 43\,k$, $y = -29\,k$, $k \in \mathbb{Z}$.

5.3 Find all the pairs of integers x and y for which

$$167\,x + 32\,y = 1.$$

Solution. We use the extended Euclid's algorithm.

1. We set $u := 167$, $x_u := 1$, $y_u := 0$, $t := 32$ $x_t := 0$, $y_t := 1$.
2. We divide u by t:

$$167 = 5 \cdot 32 + 7,$$

and we set $x_r := 1 - 5 \cdot 0$, $y_r := 0 - 5 \cdot 1$. Further, $u := 32$, $x_u := 0$, $y_u := 1$, $t := 7$, $x_t := 1$, $y_t := -5$.

3. Since $t \neq 0$, we divide u by t:

$$32 = 4 \cdot 7 + 4,$$

and we set $x_r := 0 - 4 \cdot 1$, $y_r := 1 - 4 \cdot (-5)$. Further, $u := 7$, $x_u := 1$, $y_u := -5$, $t := 4$, $x_t := -4$, $y_t := 21$.

4. Since $t \neq 0$, we divide u by t:

$$7 = 1 \cdot 4 + 3,$$

and we set $x_r := 1 - 1 \cdot (-4)$, $y_r := -5 - 1 \cdot 21$. Further, $u := 4$, $x_u := -4$, $y_u := 21$, $t := 3$, $x_t := 5$, $y_t := -26$.

5. Since $t \neq 0$, we divide u by t:

$$4 = 1 \cdot 3 + 1,$$

and we set $x_r := -4 - 1 \cdot 5$, $y_r := 21 - 1 \cdot (-26)$. Further, $u := 3$, $x_u := 5$, $y_u := -26$, $t := 1$, $x_t := -9$, $y_t := 47$.

6. Since $t \neq 0$, we divide u by t:

$$3 = 3 \cdot 1 + 0,$$

and we set $x_r := 5 - 3 \cdot (-9)$, $y_r := -26 - 3 \cdot 47$. Further, $u := 1$, $x_u := -9$, $y_u := 47$, $t := 0$, $x_t := 32$, $y_t := -167$.

Since $t = 0$, we set $\gcd(176, 32) := 1$, $x := -9$, $y := 47$.

The calculations of x_u, x_t and y_u, y_t can be arranged in the following table (which reproduces the procedure above).

	167	32
| 7	1	−5
32	0	1
$-4 \cdot 7$	−4	20
| 4	−4	21
7	1	−5
$-1 \cdot 4$	4	−21
| 3	5	−26
4	−4	21
$-1 \cdot 3$	−5	26
| 1	−9	47

We can end the table because now we know that

$$1 = -9 \cdot 167 + 47 \cdot 32,$$

and one of the solutions of $167\,x + 32\,y = 1$ is $x_0 = -9$ and $y_0 = 47$.

To get the general solution of $167\,x + 32\,y = 1$ we need to solve the homogeneous equation $167\,x + 32\,y = 0$. Since 167 and 32 are relatively prime, the general solution of the homogeneous equation is: $x = 32\,k$, $y = -167\,k$ for any $k \in \mathbb{Z}$. Hence the general solution of $167\,x + 32\,y = 1$ is

$$x = -9 + 32\,k,\ y = 47 - 167\,k \quad \text{where } k \in \mathbb{Z}.$$

5.4 Find all the solutions of the following Diophantic equation

$$712\,x + 36\,y = 2.$$

5.5 Find all the pairs of integers x and y for which

$$654\,x + 234\,y = 12.$$

5.6 Find all the pairs of integers x and y for which

$$512\,x + 355\,y = 6.$$

5.7 Find all pairs of integers x and y for which

$$32\,x + 590\,y = 16.$$

Solution. We know that the equation $32\,x + 590\,y = 16$ has a solution if and only if $\gcd(32, 590)$ divides 16. To find $\gcd(32, 590)$ it is convenient to use the Euclid's algorithm.

$$\begin{array}{rcrcr} 590 & = & 18 \cdot 32 & + & 14 \\ 32 & = & 2 \cdot 14 & + & 4 \\ 14 & = & 3 \cdot 4 & + & 2 \\ 4 & = & 2 \cdot 2 & + & 0 \end{array}$$

We have obtained $\gcd(590, 32) = 2$. Because $16 = 8 \cdot 2$, the equation has a solution.

To find on solution of the equation $32\,x + 590\,y = 16$ we extend the Euclid's algorithm.

	32	590
$\lvert$ 14	-18	1
32	1	0
$-2 \cdot 14$	36	-2
$\lvert$ 4	37	-2
14	-18	1
$-3 \cdot 4$	-111	6

Since 16 is a multiple of 4, and since $4 = 37 \cdot 32 - 2 \cdot 590$, we have got

$$16 = 148 \cdot 32 - 8 \cdot 590.$$

Hence one of solutions is $x = 148$, $y = -8$.

To get the general solution, we have to solve the homogeneous equation $32\,x + 590\,y = 0$. Since $\gcd(32, 590) = 2$, we divide the equation by 2 and get

$$16\,x + 295\,y = 0,$$

where 16 and 295 are relatively prime. So the general solution is $x = 295\,k$, $y = -16\,k$ for $k \in \mathbb{Z}$.

The general solution of $32\,x + 590\,y = 8$ is $x = 148 + 259\,k$, $y = -8 - 16\,k$, where $k \in \mathbb{Z}$.

If we do another step of the extended Euclid's algorithm we get $2 = -129\,x + 7\,590$ and hence $16 = -1032\,x + 28\,y$. with the solution $x = -1032$, $y = 28$. It is correct, indeed, $-1032 + 4 \cdot 295 = 148$ and $28 - 4 \cdot 16 = -8$.

Notice that if we were looking for one solution of the non-homogeneous equation we could divide the equation $32\,x + 590\,y = 16$ by $\gcd(32, 590) = 2$ and solve $16\,x + 295\,y = 8$ instead. But then we would need to use the Euclid's algorithm to the pair $16, 295$.

5.8 Find all pairs of integers x and y for which

$$121\,x + 531\,y = 6.$$

5.9 Find all pairs of integers x and y for which

$$141\,x + 531\,y = 6.$$

Answers

5.4 Since the greatest common divisor of 712 and 36 is 4 and 2 is not divisible by 4, the equation has no solution.

5.5 The general solution is: $x = -10 + 39\,k$, $y = 28 - 109\,k$ where $k \in \mathbb{Z}$.

5.6 The general solution is: $x = 43 - 355\,k$, $y = -62 + 512\,k$ where $k \in \mathbb{Z}$.

5.8 The general solution is: $x = 123 - 513\,k$, $y = -29 + 121\,k$ where $k \in \mathbb{Z}$.

5.9 The general solution is: $x = 49 - 177\,k$, $y = -13 + 47\,k$ where $k \in \mathbb{Z}$.

6 Tutorial 6

6.1 Find all natural numbers x, $0 \leq x < 555$ for which $233\,x \equiv 5 \pmod{555}$.

Solution. The fact that $233\,x \equiv 5 \pmod{555}$ can be reformulated as

$$233\,x = 5 + k \cdot 555, \quad \text{so} \quad 233\,x - 555\,k = 5.$$

If we substitute y for $-k$ we get the following Diophantic equation $233\,x + 555\,y = 5$. (Notice that in this case we are interested only in x, but to calculate it we need to find y as well.)

$$\begin{array}{rcrcr} 555 & = & 2 \cdot 233 & + & 89 \\ 233 & = & 2 \cdot 89 & + & 55 \\ 89 & = & 1 \cdot 55 & + & 34 \\ 55 & = & 1 \cdot 34 & + & 21 \\ 34 & = & 1 \cdot 21 & + & 13 \\ 21 & = & 1 \cdot 13 & + & 8 \\ 13 & = & 1 \cdot 8 & + & 5 \\ 8 & = & 1 \cdot 5 & + & 3 \\ 5 & = & 1 \cdot 3 & + & 2 \\ 3 & = & 1 \cdot 2 & + & 1 \\ 2 & = & 2 \cdot 1 & + & 0 \end{array}$$

We have obtained $\gcd(233, 555) = 1$. Moreover, 5 is one of the remainders. Therefore, it suffices to do the extended Euclid's algorithm till we get 5.

We obtain $x = 505$ (and $y = -212$). Since 233 and 555 are relative prime, $x = 505$ is the only solution $x = 505 + k\,555, k \in \mathbb{Z}$ which satisfies $0 \leq x < 555$.

Solution is $x = 505$.

6.2 In $\mathbf{Z}_{414}$ find all x for which

$$152\,x = 6.$$

6.3 In $\mathbf{Z}_{414}$ find all x for which

$$84\,x = 12.$$

6.4 Find the remainder when you divide

$$13^{742} - 10 \cdot 14^{521} + 22^{102}.$$

by 7.

Solution. We have $13 \equiv -1 \pmod{7}$, hence $13^{742} \equiv (-1)^{742} \pmod{7} \equiv 1 \pmod{7}$.

We have $14 \equiv 0 \pmod{7}$, hence $14^{521} \equiv 0^{742} \pmod{7} \equiv 0 \pmod{7}$.

We have $22 \equiv 1 \pmod{7}$, hence $^{102} \equiv 1^{102} \pmod{7} \equiv 1 \pmod{7}$.

Therefore, the remainder of the division is the same as the remainder of $1 - 10' \cdot 0 + 1 = 2$.

Answer: The remainder equals 2.

6.5 Find the remainder when you divide

$$4^{254} + 2 \cdot 7^{123} - 3 \cdot 11^{102}.$$

by 5.

6.6 Derive and prove criteria for divisibility by 7 and 11.

6.7 Write down the multiplication table for $(\mathbb{Z}_{10}, \odot)$.

6.8 Find all invertible elements in $(\mathbb{Z}_{11}, \odot)$ and their inverses.

Solution. Invertible elements of $\mathbb{Z}_{11}$ are all classes $[i]_{11}$ for which i and 11 are relatively prime and $0 \leq i < 11$. Since 11 is a prime number, they are all nonzero elements of $\mathbb{Z}_{11}$. Hence the set of all invertible elements is

$$\{[1]_{11}, [2]_{11}, [3]_{11}, \ldots, [9]_{11}, [10]_{11}\}.$$

Moreover,

- $[1]_{11}^{-1} = [1]_{11}$.
- Because $[2]_{11} \odot [6]_{11} = [1]_{11}$, we have $[2]_{11}^{-1} = [6]_{11}$ and $[6]_{11}^{-1} = [2]_{11}$.
- Because $[3]_{11} \odot [4]_{11} = [1]_{11}$, we have $[3]_{11}^{-1} = [4]_{11}$ and $[4]_{11}^{-1} = [3]_{11}$.
- Because $[5]_{11} \odot [9]_{11} = [1]_{11}$, we have $[5]_{11}^{-1} = [9]_{11}$ and $[9]_{11}^{-1} = [5]_{11}$.
- Because $[7]_{11} \odot [8]_{11} = [1]_{11}$ we have $[7]_{11}^{-1} = [8]_{11}$ and $[8]_{11}^{-1} = [7]_{11}$.
- Finally, $[10]_{11} \odot [10]_{11} = [1]_{11}$, $[10]_{11}^{-1} = [10]_{11}$.

6.9 Find all invertible elements in $(\mathbb{Z}_{12}, \odot)$ and their inverses.

Answers

6.2 There are two solutions, namely $x_1 = 30$, and $x_2 = 237$.

6.3 There are six solutions, namely $x_1 = 10$, $x_2 = 79$, $x_3 = 148$, $x_4 = 217$, $x_5 = 286$, and $x_6 = 355$.

6.5 The remainder equals 4.

6.7 The table is

$\odot$	$[0]_{10}$	$[1]_{10}$	$[2]_{10}$	$[3]_{10}$	$[4]_{10}$	$[5]_{10}$	$[6]_{10}$	$[7]_{10}$	$[8]_{10}$	$[9]_{10}$
$[0]_{10}$	$[0]_{10}$	$[0]_{10}$	$[0]_{10}$	$[0]_{10}$	$[0]_{10}$	$[0]_{10}$	$[0]_{10}$	$[0]_{10}$	$[0]_{10}$	$[0]_{10}$
$[1]_{10}$	$[0]_{10}$	$[1]_{10}$	$[2]_{10}$	$[3]_{10}$	$[4]_{10}$	$[5]_{10}$	$[6]_{10}$	$[7]_{10}$	$[8]_{10}$	$[9]_{10}$
$[2]_{10}$	$[0]_{10}$	$[2]_{10}$	$[4]_{10}$	$[6]_{10}$	$[8]_{10}$	$[0]_{10}$	$[2]_{10}$	$[4]_{10}$	$[6]_{10}$	$[8]_{10}$
$[3]_{10}$	$[0]_{10}$	$[3]_{10}$	$[6]_{10}$	$[9]_{10}$	$[2]_{10}$	$[5]_{10}$	$[8]_{10}$	$[1]_{10}$	$[4]_{10}$	$[7]_{10}$
$[4]_{10}$	$[0]_{10}$	$[4]_{10}$	$[8]_{10}$	$[2]_{10}$	$[6]_{10}$	$[0]_{10}$	$[4]_{10}$	$[8]_{10}$	$[2]_{10}$	$[6]_{10}$
$[5]_{10}$	$[0]_{10}$	$[5]_{10}$	$[0]_{10}$	$[5]_{10}$	$[0]_{10}$	$[5]_{10}$	$[0]_{10}$	$[5]_{10}$	$[0]_{10}$	$[5]_{10}$
$[6]_{10}$	$[0]_{10}$	$[6]_{10}$	$[2]_{10}$	$[8]_{10}$	$[4]_{10}$	$[0]_{10}$	$[6]_{10}$	$[2]_{10}$	$[8]_{10}$	$[4]_{10}$
$[7]_{10}$	$[0]_{10}$	$[7]_{10}$	$[4]_{10}$	$[1]_{10}$	$[8]_{10}$	$[5]_{10}$	$[2]_{10}$	$[9]_{10}$	$[6]_{10}$	$[3]_{10}$
$[8]_{10}$	$[0]_{10}$	$[8]_{10}$	$[6]_{10}$	$[4]_{10}$	$[2]_{10}$	$[0]_{10}$	$[8]_{10}$	$[6]_{10}$	$[4]_{10}$	$[2]_{10}$
$[9]_{10}$	$[0]_{10}$	$[9]_{10}$	$[8]_{10}$	$[7]_{10}$	$[6]_{10}$	$[5]_{10}$	$[4]_{10}$	$[3]_{10}$	$[2]_{10}$	$[1]_{10}$

6.9 Invertible elements are: $[1]_{12}$, $[5]_{12}$, $[7]_{12}$, and $[11]_{12}$. We have: $[1]_{12}^{-1} = [1]_{12}$, $[5]_{12}^{-1} = [5]_{12}$, $[7]_{12}^{-1} = [7]_{12}$, and $[11]_{12}^{-1} = [11]_{12}$

7 Tutorial 7

7.1 Find all invertible elements in $(\mathbb{Z}_{13}, \cdot, 1)$. For every invertible element a find its inverse a^{-1}.

Solution. Since 13 is a prime number, every non-zero element of $\mathbb{Z}_{13}$ is invertible. Hence the set of invertible elements is

$$\mathbb{Z}_{13} \setminus \{0\} = \{1, 2, \ldots, 12\}.$$

We have $1^{-1} = 1$ and $12^{-1} = (-1)^{-1} = -1 = 12$. To calculate 2^{-1} we can either guess for which $x \in \mathbb{Z}_{13} \setminus \{0\}$ we have $2\,x = 1$ (in $(\mathbb{Z}_{13}, \cdot, 1)$). Or we can rewrite $2\,x = 1$ in $(\mathbb{Z}_{13}, \cdot, 1)$ to $2\,x \equiv 1 \pmod{13}$ which leads to the following Diophantic equation:

$$2\,x + 13\,y = 1.$$

The equation has the following solution: $x = 7$ ($y = -1$). So $2^{-1} = 7$ and $7^{-1} = 2$.

Similarly, we get $3^{-1} = 9$, so $9^{-1} = 3$; $4^{-1} = 10$, so $10^{-1} = 4$; $5^{-1} = 8$, so $8^{-1} = 5$; and $6^{-1} = 11$, so $11^{-1} = 6$.

7.2 Given the monoid $(\mathbb{Z}_{15}, \cdot, 1)$. Find all its invertible elements and their corresponding inverses.

7.3 On the set of all real numbers $\mathbb{R}$ we define an operation $\circ$ by

$$x \circ y = \frac{x + y}{2}.$$

Decide whether $(\mathbb{R}, \circ)$ forms a semigroup.

Solution. $(\mathbb{R}, \circ)$ is not a semigroup; indeed, $(a \circ b) \circ c = a \circ (b \circ c)$ if and only if $a = c$, e.g. $2 \circ (6 \circ 3) \neq (2 \circ 6) \circ 3$.

7.4 Given a non empty set A. Define an operation $\circ$ on A by

$$x \circ y = x \quad \text{for every } x, y \in A.$$

Decide whether $(A, \circ)$ is a semigroup and whether it has a neutral element.

Solution. First we prove that $(A, \circ)$ is a semigroup: Take any $x, y, z \in A$, then $x \circ (y \circ z) = x$ (indeed, the result is always the first element). On the other hand, $(x \circ y) \circ z = x \circ z = x$. Hence, $x \circ (y \circ z) = (x \circ y) \circ z$ for every $x, y, z \in A$.

If $e \in A$ is its neutral element then $x \circ e = x = e \circ x$ for every $x \in A$. The first equation holds for any $e \in A$; indeed, $x \circ e = x$. Hence, if A has more than two elements then $(A, \circ)$ has at least two "right neutral elements", so it cannot have a neutral element.

Note, that you can get the same result from the following observation: $e \circ x = e$, hence $e \circ x = x$ if and only if $e = x$ for every $x \in A$. So, A must contain only one element which is e, the neutral element.

7.5 Given a non empty set U. Consider the set $\mathcal{P}(U)$ of all its subsets. On $A = \mathcal{P}(U)$ define two binary operations: intersection $\cap$ and union $\cup$. Decide whether $(A, \cap)$ and $(A, \cup)$ form semigroups, and whether they have a neutral element.

7.6 On the set $\mathbb{Z} \times \mathbb{Z}$ of all ordered pair of integers an operation $\circ$ is given by

$$(u, v) \circ (x, y) = (u + x, v \cdot y).$$

Decide whether $(\mathbb{Z} \times \mathbb{Z}, \circ)$ is a semigroup, whether it has a neutral element. If it is a monoid find all its invertible elements.

Solution. First we prove that $(\mathbb{Z}\times\mathbb{Z}, \circ)$ satisfies the associative law. Take any $(u, v), (x, y), (a, b) \in \mathbb{Z}\times\mathbb{Z}$. Then $(u, v)\circ((x, y)\circ(a, b)) = (u, v)\circ(x+a, y\cdot b) = (u+(x+a), v\cdot(y\cdot b)) = (u+x+a, vyb)$.

On the other hand, $((u, v)\circ(x, y))\circ(a, b) = (u+x, v\cdot y)\circ(a, b) = ((u+x)+a, (v\cdot y)\cdot b) = (u + x + a, vyb)$. So the associativity law holds.

If $(\mathbb{Z} \times \mathbb{Z}, \circ)$ has its neutral element (e, f) then for every $(u, v) \in \mathbb{Z} \times \mathbb{Z}$ it must hold

$$(u, v) \circ (e, f) = (u, v) = (e, f) \circ (u, v).$$

The left hand side is $(u+e, v\cdot f)$, the right hand side equals $(e+u, f\cdot v)$. So the only conditions (e, f) must satisfy are: $u + e = u$, $v \cdot f = v$ for every $u, v \in \mathbb{Z}$. Therefore, e must be 0, and f must be 1. We have shown that $(0, 1)$ is the neutral element of $(\mathbb{Z} \times \mathbb{Z}, \circ)$.

An element $(u, v) \in \mathbb{Z} \times \mathbb{Z}$ is invertible if and only if there exists $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ such that

$$(u, v) \circ (x, y) = (0, 1) = (x, y) \circ (u, v).$$

Hence, $u+x = 0$, and $v\cdot y = 1$ The first identity gives $x = -u$, the second identity immediately implies that $v \neq 0$. But since $\frac{1}{v}$ must be an integer, v is either 1 or -1. Let us summarize: invertible elements are $(u, 1), (u, -1)$ for an arbitrary integer u. Moreover, $(u, 1)^{-1} = (-u, 1)$, and $(u, -1)^{-1} = (-u, -1)$.

7.7 On the set $A = \mathbb{Q} \setminus \{0\}$ an operation $\star$ is given by

$$x \star y = \frac{1}{3}xy.$$

Show that $(A, \star)$ is a group.

7.8 For the group $(A, \star)$ from the exercise 7.5, decide whether the subset B forms a subsemigroup, a submonid, and a subgroup of the group $(A, \star)$ where

1. $B = \{3k\,;\, k \in \mathbb{Z}\}$,
2. $B = \{x\,;\, x \in \mathbb{Q}, x > 0\}$.

Solution. 1) To verify that $\star$ is a binary operation on B it suffices to show that $3k\star 3l$ belongs to B for any $3k, 3l \in B$. We have $3k \star 3l = \frac{1}{3}3k\,3l = 3\,kl$ and therefore belongs to B. Hence B forms a subsemigroup of $(A, \star)$.

Since $3 \in B$ (indeed, $3 = 3 \cdot 1$), B forms a submonoid of $(A, \star)$.

The set B forms a subgroup of $(A, \star)$ if and only if the inverse $(3k)^{-1}$ belongs to B for any element $3k \in B$. From the exercise 7.5 we know that $(3k)^{-1} = \frac{9}{3k}$. It is clear that not for every $k \in Z$ we have $\frac{9}{3k} \in B$. Indeed, for 6 we have $\frac{9}{6}$ is not an integer divisible by 3, hence 6^{-1} does not belong to B. We have shown that B does not form a subgroup of $(A, \star)$.

2) For two positive rational numbers x, y it holds that $\frac{1}{3}\,xy$ is again a positive rational number. Hence, B forms a subsemigroup of $(A, \star)$. Moreover, 3 is a positive rational number, hence B forms a submonoid of $(A, \star)$.

For every rational number $x > 0$ the number $x^{-1} = \frac{9}{x}$ is again a positive rational number. Hence B forms a subgroup of $(A, \star)$.

Answers

7.2 There are $\phi(15)$ invertible elements in $(\mathbb{Z}_{15}, \cdot, 1)$. Moreover, $\phi(15) = \phi(3) \cdot \phi(5) = 2 \cdot 4 = 8$. These are

$$\{1, 2, 4, 7, 8, 11, 13, 14\}.$$

We have $1^{-1} = 1$, $2^{-1} = 8$, $4^{-1} = 4$, $7^{-1} = 13$, $8^{-1} = 2$, $11^{-1} = 11$, $13^{-1} = 7$, and $14^{-1} = 14$.

7.5 $(\mathcal{P}(U), \cap)$ and $(\mathcal{P}(U), \cup)$ are semigroups. The neutral element of $(\mathcal{P}(U), \cap)$ is U, the neutral element of $(\mathcal{P}(U), \cup)$ is $\emptyset$.

7.7 It is a semigroup with its neutral element $e = 3$. Moreover, every $x \in \mathbb{Q} \setminus \{0\}$ is invertible and $x^{-1} = \frac{9}{x}$ for every x.

8 Tutorial 8

8.1 A revision exercise. Find all $x \in \mathbb{Z}_{501}$ for which

$$51\,x = 36,$$

where the multiplication is in $\mathbb{Z}_{501}$.

8.2 A revision exercise. Find the remainder when we divide the number 101^{49} by 23.

8.3 A revision exercise. On the set $A = \mathbb{Q} \setminus \{0\}$ an operation $\circ$ is given by

$$x \circ y = \frac{1}{\frac{1}{x} + \frac{1}{y}}.$$

Decide whether $(A, \circ)$ is a semigroup, and whether it has a neutral element.

8.4 Given a group $(\mathbb{Z}_{11}^\star, \cdot, 1)$ of all invertible elements of $(\mathbb{Z}_{11}, \cdot, 1)$. Show that it is a cyclic group. Find at least one generating element. How many generating elements $(\mathbb{Z}_{11}^\star, \cdot, 1)$ has?

Solution. A group is cyclic if and only if it has a generating element; i.e. an element $a \in \mathbb{Z}_{11}^\star$ such that any element of $\mathbb{Z}_{11}^\star$ is a power of a. Let us try "small"elements a (the reason for that is that it is easier to calculate the powers of small number than "bigger"ones).

For $a = 2$ we have

- $a^1 = 2$;
- $a^2 = 2^2 = 4$;
- $a^3 = 2^3 = 8 = -3$;
- $a^4 = 2^4 = 5$;
- $a^5 = 2^5 = 10 = -1$;
- $a^6 = 2^6 = -2 = 9$;
- $a^7 = 2^7 = -4 = 7$;
- $a^8 = 2^8 = 3$;
- $a^9 = 2^9 = -5 = 6$;
- $a^{10} = 2^{10} = 1$.

We can see that all 10 elements of $\mathbb{Z}_{11}^\star$ are powers of 2, hence 2 is a generating element of $(\mathbb{Z}_{11}^\star, \cdot 1)$. Therefore, $(\mathbb{Z}_{11}^\star, \cdot 1)$ is a cyclic group.

Since any element $b = 2^i$ with $\gcd(i, 10) = 1$ is also a generating element of $(\mathbb{Z}_{11}^\star, \cdot 1)$, there are $\phi(10) = 4$ generating elements. The generating elements are $6 = 2^9$, $7 = 2^7$ a $8 = 2^3$.

Let us mention that we do not have to calculate all the powers of 2. Indeed, the order of any element of a finite group divides the order of the group. Hence, $a \in \mathbb{Z}_{11}^\star$ can have orders only one of the numbers 1, 2, 5, 10 (which are divisors of $10 = |\mathbb{Z}_{11}^\star|$). Therefore, if $a \neq 1$ satisfies $a^2 \neq 1$, $a^5 \neq 1$, then a is a generating element of $(\mathbb{Z}_{11}^\star, \cdot 1)$.

8.5 Given a group $(\mathbb{Z}_8^\star, \cdot, 1)$ of all invertible elements of $(\mathbb{Z}_8, \cdot, 1)$. Decide whether it is a cyclic group.

Solution. We have $a \in \mathbb{Z}_8^\star$ if and only if $\gcd(a, 8) = 1$. Hence $\mathbb{Z}_8^\star = \{1, 3, 5, 7\}$. Let us calculate orders of all elements of $\mathbb{Z}_8^\star$.

- The order of 1 is 1.
- Since $3^2 = 1$, the order of 3 is 2.

- Since $5^2 = 1$, the order of 5 is 2.
- Since $7^2 = 1$, the order of 7 is 2.

Hence, all elements of $\mathbb{Z}_8^\star$ different from 1 have order 2, no one has order 4. Therefore, $(\mathbb{Z}_8^\star, \cdot, 1)$ is not cyclic.

Notice that $(\mathbb{Z}_8^\star, \cdot, 1)$ has 5 subgroups: namely, $\{1\}$, $\{1,3\}$, $\{1,5\}$, $\{1,7\}$, and $\mathbb{Z}_8^\star$. Unlike a cyclic group $(\mathbb{Z}_8^\star, \cdot, 1)$ has three subgroups for order 2.

8.6 Given a group $(\mathbb{Z}_{17}^\star, \cdot, 1)$. Find the order of 2. Is 2 a generating element? Write down $\langle 2 \rangle$ in $\mathbb{Z}_{17}^\star$.

Solution. Since the group $(\mathbb{Z}_{17}^\star, \cdot, 1)$ has 16 elements, its elements have orders from the set of all divisors of 16, i.e. from the set $\{1, 2, 4, 8, 16\}$. We have $2^2 = 4$, $2^4 = 16 = -1$, hence $2^8 = 1$. Therefore, the order of 2 is 8. Since 2 has order 8, 2 is not a generator.

Moreover, $\langle 2 \rangle = \{2^i \mid 1 = 1, 2, 3, 4, 5, 6, 7, 8\} = \{1, 2, 4, 8, 9, 13, 15, 16\}$.

8.7 Given a group $(\mathbb{Z}_{17}^\star, \cdot, 1)$. Find all its generating elements.

Solution. From exercise 8.6 we know that $\langle 2 \rangle \neq \mathbb{Z}_{17}^\star$. Hence no $a \in \langle 2 \rangle$ is a generating element. Let us compute powers of 3:

- $3^2 = 9 \neq 1$;
- $3^4 = 13 = -4 \neq 1$;
- $3^8 = 16 = -1 \neq 1$.

Hence, the order of 3 is 16 and 3 is a generating element of $(\mathbb{Z}_{17}^\star, \cdot, 1)$.

There are $\phi(16) = 8$ generating elements; indeed, for every i relatively prime to 16, the element 3^i is a generating element. Hence, all generating elements are $3^1 = 3$, $3^3 = 10$, $3^5 = 5$, $3^7 = 11$, $3^9 = 14$, $3^{11} = 7$, $3^{13} = 12$ a $6 = 3^{15}$.

8.8 Given a group $(\mathbb{Z}_{17}^\star, \cdot, 1)$. Find all its subgroups.

Solution. Since the group $(\mathbb{Z}_{17}^\star, \cdot, 1)$ is a cyclic group with 16 elements, for every divisor d of 16 there is one subgroup of d elements.

1. For $d = 1$, we have the subgroup $\{1\}$.
2. For $d = 2$, we have the subgroup $\{1, -1\} = \{1, 16\}$; indeed, $16 = -1$ has order 2.
3. For the subgroup with 4 elements we need an element of order 4. Since 2 has the order 8, $2^2 = 4$ has the order 4. Hence $\langle 4 \rangle = \{4, 4^2, 4^3, 4^4\}$ is the subgroup of order 4. Moreover, $4^2 = 16 = -1$, $4^3 = -4 = 13$, and $4^4 = 1$. Hence $\langle 4 \rangle = \{1, 4, 13, 16\}$.
4. We already know that $\langle 2 \rangle$ has 8 elements, so the set $\{1, 2, 4, 8, 9, 13, 15, 16\}$ forms a subgroup with 8 elements.
5. The only subgroup of $(\mathbb{Z}_{17}^\star, \cdot, 1)$ with 16 elements is $(\mathbb{Z}_{17}^\star, \cdot, 1)$ itself.

We have shown that $\{1\}$, $\{1, 16\}$, $\{1, 4, 13, 16\}$, $\{1, 2, 4, 8, 9, 13, 15, 16\}$ and $\mathbb{Z}_{17}^\star$ are all subgroups of $(\mathbb{Z}_{17}^\star, \cdot, 1)$.

Answers

8.1 $x_1 = 40$, $x_2 = 207$ a $x_3 = 374$

8.2 The remainder is 8.

8.3 The operation $\circ$ is an operation on the set $A = \mathbb{Q} \setminus \{0\}$ because for rational numbers x, y, $x \neq 0 \neq y$, the number $\frac{1}{\frac{1}{x}+\frac{1}{y}}$ is again a rational non-zero number.

Let us calculate

$$x \circ (y \circ z) = x \circ \frac{1}{\frac{1}{y}+\frac{1}{z}} = \frac{1}{\frac{1}{x}+\frac{1}{\frac{1}{y}+\frac{1}{z}}} = \frac{1}{\frac{1}{x}+\frac{1}{y}+\frac{1}{z}}.$$

On the other hand,

$$(x \circ y) \circ z = \frac{1}{\frac{1}{x}+\frac{1}{y}} \circ z = \frac{1}{\frac{1}{\frac{1}{x}+\frac{1}{y}}+\frac{1}{z}} = \frac{1}{\frac{1}{x}+\frac{1}{y}+\frac{1}{z}}.$$

Hence, $x \circ (y \circ z) = (x \circ y) \circ z$ and the operation $\circ$ satisfies the associativity law. Therefore, $(A, \circ)$ is a semigroup.

If e is a neutral element of $(A, \circ)$ then for every rational number $x \neq 0$ it must hold that

$$x \circ e = x = e \circ x.$$

So, $\frac{1}{\frac{1}{x}+\frac{1}{e}} = x$ for every x; which means that $\frac{1}{x} = \frac{1}{x} + \frac{1}{e}$. Hence $\frac{1}{e} = 0$, and this holds for no rational number. Therefore the neutral element does not exist.

9 Tutorial 9

Midterm test.

9.1 Calculate 5^{676} in $(\mathbb{Z}_{306}, \cdot, 1)$ and use it to find all elements $x \in \mathbb{Z}_{306}$ for which

$$5^{676} \cdot x = 3\,(2x+1) \quad \text{in } (\mathbb{Z}_{306}, \cdot, 1).$$

Solution. We know that if a and n are relatively prime then $a^{\phi(n)} = 1$ in $(\mathbb{Z}_n, \cdot, 1)$. Since 5 and 306 are relatively prime and since

$$\phi(306) = \phi(2 \cdot 9 \cdot 17) = \phi(2) \cdot \phi(3^2) \cdot \phi(17) = 6 \cdot 16 = 96,$$

we have $5^{96} = 1$. So

$$5^{676} = 5^{7 \cdot 96 + 4} = 5^4.$$

Further, $5^4 = 13$ in $\mathbb{Z}_{306}$. Therefore, we obtain the following equation

$$13\,x = 6\,x + 3, \;\text{ hence }\; 7\,x = 3.$$

Solving the equation above, we get $x = 219$.

9.2 In $\mathbb{Z}_{148}$ the following equation with parameter p is given

$$p\,x - 5^{509} = 9\,x + 7.$$

a) Find all parameters p for which the equation above has a unique solution.

b) Solve the equation above for three such parameters (from a)).

Solution.
a) The equation above can be rewritten

$$(p-9)\,x = 5^{509} + 7,$$

and it has a unique solution if and only if $(p-9)$ is invertible in $(\mathbb{Z}_{148}, \cdot, 1)$. There are $\phi(148)$ distinct elements in $(\mathbb{Z}_{148}, \cdot, 1)$ that are invertible. Moreover,

$$\phi(148) = \phi(4) \cdot \phi(37) = 2 \cdot 36 = 72.$$

Hence, there are 72 distinct parameters in $\mathbb{Z}_{148}$ for which the above equation has a unique solution.

b) Since 5 and 148 are relatively prime, $5^{72} = 1$ in $\mathbb{Z}_{148}$. Therefore,

$$5^{509} = 5^{72 \cdot 7 + 5} = 5^5 = 17.$$

Therefore, the equation above is $(p-9)\,x = 24$ and the unique solutions will be $x = (p-9)^{-1} \cdot 24$ in $(\mathbb{Z}_{148}, \cdot, 1)$.

For example, we choose the following three parameters so that

$$p_1 - 9 = 1,\; p_2 - 9 = -1,\; p_3 - 9 = 3.$$

Hence, $p_1 = 10$, $p_2 = 8$, and $p_3 = 12$.

Therefore, for $p_1 = 10$ we get $x_1 = 24$, and for $p_2 = 8$ we get $x_2 = -24 = 124$.

For $p_3 = 12$ the easiest way is: since $3\,x = 24$ and 3^{-1} exists in $(\mathbb{Z}_{148}, \cdot, 1)$ we can cancel by 3 and get $x = 8$. Hence, $x_3 = 8$.

10 Tutorial 10

10.1 Given a Boolean algebra B with operations $\wedge$, $\vee$, complement $\overline{a}$ of a, the smallest element $\mathbf{0}$, and the greatest element $\mathbf{1}$. Show that for every $a, b \in B$ it holds that

$$\text{if } a \sqsubseteq b \text{ then } a \wedge \overline{b} = \mathbf{0} \text{ and } \overline{a} \vee b = \mathbf{1}.$$

Solution. We show the first part, the second part can be proved analogously.

We have $a \sqsubseteq b$ if and only if $a \wedge b = a$. Therefore,

$$a \wedge \overline{b} = (a \wedge b) \wedge \overline{b} = a \wedge (b \wedge \overline{b}) = a \wedge \mathbf{0} = \mathbf{0}.$$

10.2 Given a Boolean algebra B with operations $\wedge$, $\vee$, complement $\overline{a}$ of a, the smallest element $\mathbf{0}$, and the greatest element $\mathbf{1}$. Show that for every $a, b \in B$ we have

$$a \sqsubseteq b \quad \text{if and only if} \quad \overline{b} \sqsubseteq \overline{a}.$$

10.3 Given a Boolean algebra B with operations $\wedge$, $\vee$, complement $\overline{a}$ of a, the smallest element $\mathbf{0}$, and the greatest element $\mathbf{1}$. Show that for every $a, b, c \in B$ we have

$$\text{if } a \sqsubseteq b \text{ then } a \wedge c \sqsubseteq b \wedge c, \quad a \vee c \sqsubseteq b \vee c.$$

Solution. We show that $a \wedge c \sqsubseteq b \wedge c$; the other equality can be proved similarly.

We know that $a \sqsubseteq b$ if and only if $a \wedge b = a$. Let us calculate

$$(a \wedge c) \wedge (b \wedge c) = (a \wedge b) \wedge c = a \wedge c.$$

Therefore, $a \wedge c \sqsubseteq b \wedge c$ holds.

10.4 Given a Boolean algebra B with operations $\wedge$, $\vee$, complement $\overline{a}$ of a, the smallest element $\mathbf{0}$, and the greatest element $\mathbf{1}$. Define a new operation $\mid$ on B by

$$a \mid b = \overline{a} \vee \overline{b}.$$

Show that

$$a \vee b = (a \mid a) \mid (b \mid b) \quad \text{and} \quad a \wedge b = (a \mid b) \mid (a \mid b).$$

Solution. We show the first part.

Let us calculate

$$(a \mid a) \mid (b \mid b) = (\overline{a} \vee \overline{a}) \mid (\overline{b} \vee \overline{b}) = \overline{a} \mid \overline{b} = \overline{\overline{a}} \vee \overline{\overline{b}} = a \vee b.$$

10.5 Draw a tree T on the set of vertices $V = \{1, \ldots, 8\}$.

10.6 Draw all different trees with 5 vertices. (Two trees are the same if they differ only in names of vertices.)

Solution. Since the sum of degrees must be 8 and since there are at least two vertices of degree one, the sum of degrees of 3 vertices must be 6. One possibility is $2+2+2$ which gives a path; the second possibility is $1+2+3$, and the last possibility is $1+1+4$. Since for every case there is only one tree with the prescribed degrees, there are only these three different trees.

10.7 Draw a simple undirected graph G which has 8 vertices, 10 edges, and 2 components of connectivity.

10.8 Given a tree T on the set of vertices $V = \{1, \ldots, 6\}$. If G is a graph obtained from T by adding 2 edges (between vertices from V) how many circuits G can have? Give the smallest and the biggest number of circuits.

Answers

10.8 A tree with 2 added edges can have either 2 or 3 circuits. Indeed, the first edge closes just one circuit, say C_1. The second edge can close either a circuit C_2 which is vertex disjoint with C_1, or C_2 can have a common edge with C_1. In the first case, the graph contains two circuits, in the second case three.

11 Tutorial 11

11.1 Find a minimal spanning tree in the undirected graph given by the following matrix of weights

$$\begin{pmatrix} - & 9 & 13 & 5 & - & 7 & - & 9 \\ 9 & - & 13 & - & 4 & - & - & 14 \\ 13 & 13 & - & 6 & 5 & 4 & 9 & 2 \\ 5 & - & 6 & - & 4 & - & - & - \\ - & 4 & 5 & 4 & - & 5 & - & 1 \\ 7 & - & 4 & - & 5 & - & 15 & 8 \\ - & - & 9 & - & - & 15 & - & 7 \\ 9 & 14 & 2 & - & 1 & 8 & 7 & - \end{pmatrix}$$

Solution. First we sort the edges (we state the weight of an edge in the brackets)
$e_1 = \{5,8\}\,(1)$, $e_2 = \{3,8\}\,(2)$, $e_3 = \{2,5\}\,(4)$, $e_4 = \{3,6\}\,(4)$, $e_5 = \{4,5\}\,(4)$, $e_6 = \{1,4\}\,(5)$, $e_7 = \{3,5\}\,(5)$, $e_8 = \{5,6\}\,(5)$, $e_9 = \{3,4\}\,(6)$, $e_{10} = \{1,6\}\,(7)$, $e_{11} = \{7,8\}\,(7)$, $e_{12} = \{6,8\}\,(8)$, $e_{13} = \{1,2\}\,(9)$, $e_{14} = \{1,8\}\,(9)$, $e_{15} = \{3,7\}\,(9)$, $e_{16} = \{1,3\}\,(13)$, $e_{17} = \{2,3\}\,(13)$, $e_{18} = \{2,8\}\,(14)$, $e_{19} = \{6,7\}\,(15)$.
Put $L = \emptyset$.

Now we will go through edges in the given order and include e_i into L if and only if it does not close a circuit.

1. e_1 does not close a circuit, hence $L := \{\{5,8\}\}$.
2. e_2 does not close a circuit, hence $L := \{\{5,8\},\{3,8\}\}$.
3. e_3 does not close a circuit, hence $L := \{\{5,8\},\{3,8\},\{2,5\}\}$.
4. e_4 does not close a circuit, hence $L := \{\{5,8\},\{3,8\},\{2,5\},\{3,6\}\}$.
5. e_5 does not close a circuit, hence $L := \{\{5,8\},\{3,8\},\{2,5\},\{3,6\},\{4,5\}\}$.
6. e_6 does not close a circuit, hence $L := \{\{5,8\},\{3,8\},\{2,5\},\{3,6\},\{4,5\},\{1,4\}\}$.
7. e_7 closes a circuit formed by e_1, e_2 and e_7, hence L is the same as in 6.
8. e_8 closes a circuit formed by e_1, e_2, e_4 and e_8, hence L is the same as in 6.
9. e_9 closes a circuit formed by e_5, e_1, e_2 and e_9, hence L is the same as in 6.
10. e_{10} closes a circuit formed by e_6, e_5, e_1, e_2, e_4 and e_{10}, hence L is the same as in 6.
11. e_{11} does not close a circuit, hence $L := \{\{5,8\},\{3,8\},\{2,5\},\{3,6\},\{4,5\},\{1,4\},\{7,8\}\}$.

Since L contains $8-1=7$ edges, we have

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

is the set of edges of a minimal spanning tree of G. The weight (price) of L is

$$c(L) = 1+2+4+4+4+5+7 = 27.$$

11.2 Find a minimal spanning tree in the undirected graph given by the following matrix of weights

$$\begin{pmatrix} - & 5 & 9 & 3 & 2 & 5 & 1 \\ 5 & - & 18 & 7 & 19 & 1 & 7 \\ 9 & 18 & - & 6 & 19 & 10 & 3 \\ 3 & 7 & 6 & - & 14 & 8 & 9 \\ 2 & 19 & 19 & 14 & - & 7 & 8 \\ 5 & 1 & 10 & 8 & 7 & - & 4 \\ 1 & 7 & 3 & 9 & 8 & 4 & - \end{pmatrix}$$

11.3 Find an example of an undirected weighted graph which has a unique minimal spanning tree, or show that such a graph does not exist.

11.4 Find an example of an undirected weighted graph which has precisely two minimal spanning trees, or show that such a graph does not exist.

11.5 Given a directed graph $G = (V, E)$, $V = \{1, \ldots, 12\}$, E is given by the following table (u is the initial vertex of e, v is the terminal vertex of e).

u	1	1	2	4	4	4	4	4	4	5	5	6	6	7	7	8	8	10	10	11	11	11	12
v	2	9	9	2	5	7	9	10	12	3	10	5	10	1	2	6	9	2	9	1	2	5	2

Decide whether G has a topological sort or not. If the answer is yes, find one topological sort of vertices.

Solution. The graph G is acyclic if and only if it has a topological sort of vertices. We will use the algorithm for finding a topological sort of vertices; if we succeed in sorting all vertices, the graph is acyclic; if not, the graph is not acyclic.

First, we calculate the in-degrees of vertices of G. We get

v	1	2	3	4	5	6	7	8	9	10	11	12
$d^-(v)$	2	6	1	0	3	1	1	0	5	3	0	1

The set M contains all vertices with in-degree 0; therefore $M := \{4, 8, 11\}$. We set $i := 1$.

Since M is non-empty, we choose an arbitrary element from M, say 4, and put $v_1 = 4$.

Now, for every edges with initial vertex 4 we decrease the in-degree of the terminal vertex w by 1. If we get $d^-(w) = 0$ we insert w in M.

Hence,

$$d^-(2) = 5, d^-(5) = 2, d^-(7) = 0, d^-(9) = 4, d^-(10) = 2, d^-(12) = 0,$$

and

$$M := \{8, 11, 7, 12\}, i := 2.$$

Since M is non-empty, we choose an arbitrary element from M, say 8, and put $v_2 = 8$.

Now, for every edges with initial vertex 8 we decrease the in-degree of the terminal vertex w by 1. If we get $d^-(w) = 0$ we insert w in M.

Hence,

$$d^-(6) = 0, d^-(9) = 3, \quad \text{and} \quad M := \{11, 7, 12, 6\}, \quad i := 3.$$

Similarly, we put $v_3 = 11$. Hence,

$$d^-(1) = 1, d^-(2) = 4, d^-(5) = 1, \quad \text{and} \quad M := \{7, 12, 6\}, \quad i := 4.$$

We put $v_4 = 7$. Hence,

$$d^-(1) = 0, d^-(2) = 3, \quad \text{and} \quad M := \{12, 6, 1\}, \quad i := 5.$$

We put $v_5 = 12$. Hence,

$$d^-(2) = 2, \quad \text{and} \quad M := \{6, 1\}, \quad i := 6.$$

We put $v_6 = 6$. Hence,

$$d^-(5) = 0, d^-(10) = 1, \quad \text{and} \quad M := \{1, 5\}, \quad i := 7.$$

We put $v_7 = 1$. Hence,

$$d^-(2) = 1, d^-(10) = 1, \quad \text{and} \quad M := \{5\}, \quad i := 8.$$

We put $v_8 = 5$. Hence,

$$d^-(3) = 0, d^-(10) = 0, \quad \text{and} \quad M := \{3, 10\}, \;\; i := 9.$$

We put $v_9 = 3$. Since there is not edge with initial vertex 3, we get

$$M := \{10\} \quad \text{and} \quad i := 10.$$

We put $v_{10} = 10$. Hence,

$$d^-(2) = 0, d^-(9) = 1, \quad \text{and} \quad M := \{2\}, \;\; i := 11.$$

We put $v_{11} = 2$. Hence,

$$d^-(9) = 0, \quad \text{and} \quad M := \{9\}, \;\; i := 12.$$

We put $v_{12} = 9$. Hence,

$$M := \emptyset \quad \text{and} \quad i := 13.$$

Since $M = \emptyset$, the algorithm terminates. The sequence which was found is

$$v_1 = 4, v_2 = 8, v_3 = 11, v_4 = 7, v_5 = 12, v_6 = 6, v_7 = 1, v_8 = 5, v_9 = 3, v_{10} = 10, v_{11} = 2, v_{12} = 9$$

is a topological sort of vertices. Therefore, the graph G is acyclic.

11.6 Given a directed graph $G = (V, E)$, $V = \{1, \ldots, 12\}$, E is given by the following table (u is the initial vertex of e, v is the terminal vertex of e).

u	1	3	3	3	3	4	5	5	5	6	6	6	6	6	6	6	8	8	8	9	12	12	12	12
v	4	4	7	9	10	7	2	4	11	1	3	4	5	7	9	12	9	10	11	11	1	2	3	8

Decide whether G has a topological sort or not. If the answer is yes, find one topological sort of vertices.

11.7 Given a directed graph $G = (V, E)$, $V = \{1, \ldots, 12\}$, E is given by the following table (u is the initial vertex of e, v is the terminal vertex of e).

u	1	2	2	2	2	2	3	4	4	5	5	6	6	6	6	6	7	7	7	8	11	11	12
v	3	1	6	7	9	12	4	8	11	3	8	4	7	9	10	12	1	5	10	3	3	10	8

Decide whether G has a topological sort or not. If the answer is yes, find one topological sort of vertices.

11.8 Draw a simple directed acyclic graph which has 9 vertices, and 15 edges.

Answers

11.2 The set of edges of a minimal spanning tree is

$$L = \{\{1, 7\}, \{2, 6\}, \{1, 5\}, \{1, 4\}, \{3, 7\}, \{6, 7\}\}.$$

The weight (price) of L is

$$c(L) = 1 + 1 + 2 + 3 + 3 + 4 = 14.$$

11.3 For example, the graph from 11.2 has a unique minimal spanning tree.

11.4 The following weighted graph (given by its matrix of weights) has precisely two minimal spanning trees.

$$\begin{pmatrix} - & 1 & - & - \\ 1 & - & 1 & 2 \\ - & 1 & - & 2 \\ - & 2 & 2 & - \end{pmatrix}$$

Indeed, $L_1 = \{\{1,2\},\{2,3\},\{3,4\}\}$ and $L_2 = \{\{1,2\},\{2,3\},\{2,4\}\}$ are the only minimal spanning trees (with $c(L_1) = c(L_2) = 4$).

11.6 The graph G is acyclic, since it has a topological sort of vertices, one of them is

$v_1 = 6, v_2 = 5, v_3 = 12, v_4 = 1, v_5 = 2, v_6 = 3, v_7 = 8, v_8 = 4, v_9 = 9, v_{10} = 10, v_{11} = 7, v_{12} = 11.$

11.7 The graph G is not acyclic; for example, edges $(3,4)$, $(4,8)$, and $(8,3)$ form a cycle.

Notice, that when constructing a topological sort, the algorithm halts when $v_1 = 2$, $v_2 = 6$, $v_3 = 7$, $v_4 = 9$, $v_5 = 12$, $v_6 = 5$, and $v_7 = 1$. After that, the set M is empty and not all vertices were sorted.

12 Tutorial 12

12.1 Give an example of a simple directed graph which has 9 vertices, 12 directed edges, 2 components of connectivity, and 4 strongly connected components.

12.2 Give an example of a simple directed graph which has 9 vertices, 12 directed edges, 2 components of connectivity, and 2 strongly connected components.

12.3 Is it possible that a simple directed graph has more connected components than strongly connected components?

12.4 Let G be a simple strongly connected directed graph without loops, which has n vertices. Give the smallest and biggest numbers of edges that G can have. Justify your answers.

12.5 Given a simple directed graph G with the set of vertices $V = \{1, \dots, 8\}$, and the set of edges is given by the following table.

IV	1	1	1	2	2	3	3	3	4	5	6	6	7	8
TV	2	3	5	1	3	1	4	6	1	2	3	7	8	6

Decide whether G is an Euler graph; in other words, either find a closed directed Euler trail, or justify that such trail does not exist.

Solution. First of all we calculate the in-degrees and out-degrees of all vertices in G. If there is a vertex v for which $d^+(v) \neq d^-(v)$, then a closed directed Euler trail does not exist.

We have

	1	2	3	4	5	6	7	8
$d^-(v)$	3	2	3	1	1	2	1	1
$d^+(v)$	3	2	3	1	1	2	1	1

Since $d^+(v) = d^-(v)$ for all vertices of G, we can start the algorithm for finding a closed directed Euler trail.

We start in an arbitrary vertex, say 1, and we randomly form a maximal trail T (the trail T will be given as a sequence of edges only). Then T is

$$T := (1,2), (2,1), (1,3), (3,1), (1,5), (5,2), (2,3), (3,4), (4,1).$$

The trail T cannot be extended, since there is no edge with its initial vertex 1 which is not contained in T.

Since T does not contain all edges of G, there must be a vertex w on T for which not all edges incident to w are contained in T. (If this was not true, then G would be disconnected and a closed Euler trail would not exist). All edges incident to 1 and 2 are contained in T, hence the first vertex with edges incident to it and not in T is 3. We randomly form a directed trail T_1 starting in 3 and containing only edges not in T. T_1 is

$$T_1 := (3,6), (6,3).$$

We insert T_1 into T and get a new closed trail T:

$$T := (1,2), (2,1), (1,3), (3,6), (6,3), (3,1), (1,5), (5,2), (2,3), (3,4), (4,1).$$

Now, all edges incident to 1,2,3 are contained in T, and we choose 6 with the edge $(6,7)$ not in T. We randomly construct a maximal trail T_2 starting in 6 consisting of edges not in T. We have

$$T_2 := (6,7),(7,8),(8,6).$$

We insert T_2 in T and get a new trail

$$T := (1,2),(2,1),(1,3),(3,6),(6,7),(7,8),(8,6),(6,3),(3,1),(1,5),(5,2),(2,3),(3,4),(4,1).$$

Now, T contains all edges of G, hence it is a closed directed Euler trail (and G is an Euler graph).

12.6 Given a simple directed graph G with the set of vertices $V = \{1,\ldots,8\}$, and the set of edges is given by the following table.

IV	1	1	1	2	3	4	5	5	6	7	7	8	8
TV	5	6	8	1	7	2	1	2	8	1	5	3	7

Decide whether G contains an open directed Euler trail, or justify that such trail does not exist.

12.7 Give an example of a directed graph with 10 vertices and 12 edges that

1. is a Hamiltonian graph;
2. is not a Hamiltonian graph.

Answers

12.3 It is not possible.

12.4 The smallest number is n, the biggest number is $n\,(n-1)$.

12.6 Yes, there exists an open directed Euler trail T.

$$T := (4,2),(2,1)(1,5),(5,1),(1,6)(6,8),(8,3),(3,7),(7,1),(1,8),(8,7),(7,5),(5,2).$$

13 Tutorial 13

13.1 There are 150 male students and 40 female students in a class. A delegation of 4 persons will be chosen.

(1) How many ways such a delegation can be chosen?

(2) How many ways a delegation can be chosen if a delegation must contain three male students and one female student?

(3) How many ways a delegation and its spokesperson can be chosen if a delegation must contain three male students and one female student?

Solution.

(1) Because there is no restriction on a delegation, we have altogether $150 + 40 = 190$ students and we choose 4 element subset of it. Hence the number of distinct choices is

$$\binom{190}{4} = 52\,602\,165.$$

(2) We choose first a group of 3 male students and independently a female student. So, the number of distinct delegations is

$$\binom{150}{3} \cdot 40 = 551\,300 \cdot 40 = 22\,052\,000.$$

(3) We can calculate the number by two different ways:

a) For each delegation from the part 2) there are 4 possibilities how to choose its spokesman. Hence we have

$$4 \cdot \left(\binom{150}{3} \cdot 40\right) = 4 \cdot 22\,052\,000 = 88\,208\,000.$$

b) Directly; we first choose a spokesman and then the remaining members of the delegation. We should distinguish between delegations where its spokesman is a male student, and delegations where its spokesman is a female student. Hence, we have

$$150 \cdot 40 \cdot \binom{149}{2} + 40 \cdot \binom{150}{3} = 66\,156\,000 + 22\,052\,000 = 88\,208\,000.$$

13.2 We have 3 cakes with poppy seed and 7 cakes with white cheese. We want to choose 8 cakes. How many ways it can be done if the order is not important?

13.3 How many different ways there are if we want to choose 12 apples from a basket with 20 red apples, 20 green apples, and 20 yellow apples, if at least 3 apples must be chosen of each sort?

13.4 Consider numbers $1, 2, \ldots, n$ where $n \geq 11$. How many ways are there to choose five different numbers from them in such a way that the second largest number number does not exceed 10?

13.5 Prove that for every $n > 0$ it holds that

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \ldots + \binom{n}{n-1} + \binom{n}{n} = 2^n.$$

Solution. The formula can be proved directly using the definition of binomial coefficients, but there is a combinatorial proof as well.

The number $\binom{n}{i}$ is the number of all subsets of the set $\{1, 2, \ldots, n\}$ having i elements. So

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \ldots + \binom{n}{n-1} + \binom{n}{n}$$

is the number of all subsets of the set $\{1, 2, \ldots, n\}$. And we know that there are 2^n subsets of it.

13.6 Prove that for any n, k for which $n \geq k > 2$ it holds that

$$\binom{n}{k} = \binom{n-2}{k} + 2\binom{n-2}{k-1} + \binom{n-2}{k-2}.$$

Solution. We have

$$\binom{n-2}{k} + 2\binom{n-2}{k-1} + \binom{n-2}{k-2} = \left(\binom{n-2}{k} + \binom{n-2}{k-1}\right) + \left(\binom{n-2}{k-1} + \binom{n-2}{k-2}\right) =$$

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

13.7 In a class of all boys, 13 boys like to play soccer, 17 boys like biking, and 8 boys like hiking. The number of boys who like both soccer and biking is 10, the number of those who like soccer and hiking is 2, and the number of boys who like both biking and hiking is 4. There is one boy who likes all three activities, and 2 boys from the class do not like any of these activities. How many boys there are in the class?

13.8 Suppose that 19 positive even numbers were chosen all of them smaller than 500. Show that there will be at least two numbers whose difference is at most 26.

Solution. Assume that we have chosen 19 even numbers from numbers $2, \ldots, 498$. Consider the smallest chosen number k. If all differences of two numbers chosen are at least 28 then the biggest number must be $k + 18 \cdot 28$, which is $k + 504$ and it is more than 500 (as $k \geq 2$). A contradiction.

13.9 A drawer contains 5 pairs of socks of gray color, 4 pairs of socks of black color, and 4 pairs of socks of dark blue color.

1) How many single socks do we have to take out of the drawer to make sure that we have two socks of the same color?

2) How many single socks do we have to take out of the drawer to make sure that we have two socks of different colors?

Answers

13.2 There are only 3 ways how to choose 8 cakes; indeed, either we take 3 cakes with poppy seed and remaining 5 cakes with white cheese, or 2 cakes with poppy seed and 6 cakes with white cheese, or 1 cake with poppy seed and 7 cakes with white cheese.

13.3 There are 10 different ways how to choose 12 apples. Indeed, we only choose 3 apples (9 apples are there because from each sort there must be at least 3 apples). This can be done in 10 different ways.

13.4 A choice satisfying conditions above either does not contain a number greater than 10 (and there are $\binom{10}{5}$ such choices), or it has the biggest number greater than 10 and the remaining numbers are at most 10 (and there are $(n-10)\cdot\binom{10}{4}$ such choices).

Therefore, we have

$$\binom{10}{5}+(n-10)\cdot\binom{10}{4}=252+(n-10)\,210=210\,n-1848.$$

13.7 There are 25 boys in the class.

13.9

1) If we take out of the drawer 4 single socks then two of them must have the same color.
2) If we take out of the drawer 6 single socks then two of them must have different color. (5 is not sufficient since they may all be grey.)