

Task 1. Sets, Relations, Functions, and Proof Patterns.....33 Points

a) **Short Questions.** Each correct answer gives the number of points indicated in the brackets. No justification is required.

- 1.) Let $A = \{\{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\{\emptyset\}\}\}$. In the following list, **circle** all sets x such that $x \in A$, and **cross** all sets y such that $y \subseteq A$. (1 Point)

$\{\emptyset\}$

$\{\{\emptyset\}, \{\emptyset\}\}$

\emptyset

$\{\{\{\emptyset\}\}, \emptyset\}$

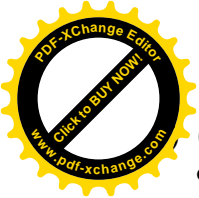
- 2.) Let A, B, C be sets and let $X = (A \cap B) \setminus ((A \cup B) \cap C)$. Write an expression for X using (not necessarily all) set operations \cup, \cap , and \setminus in which A, B, C appear *at most once*. (1 Point)

- 3.) Let A, B, C be sets such that $|(A \cup B) \times (C \cup B)| = 3$ and $A \cap B = \emptyset$. Write all the possible values of $|A| + |C|$. (2 Points)

- 4.) Let $A = \{a, b, c, d\}$. Find the smallest relation ρ on A such that $\{(a, b), (d, b)\} \subseteq \rho$ and both $\rho = \hat{\rho}$ and $\rho^2 \subseteq \rho$. (2 Points)

- 5.) Consider the poset $(\{1, 2, 3, 4, 8, 9, 24, 36\}; |)$ and let $S = \{2, 3\}$. Write all upper bounds of S in A . If there are least upper bounds of S in A , identify them, or else, write that none exist. (2 Points)

- b) (★) Let X be a set and let ρ and σ be equivalence relations on X . **Prove or disprove** that $\rho \cap \sigma$ is an equivalence relation. (4 Points)



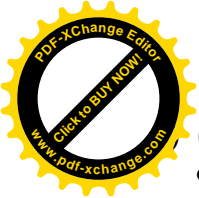
(★) Let A, B be non-empty sets such that there exists an injective function $f : A \rightarrow B$. **Prove or disprove** that there exists a surjective function $g : B \rightarrow A$. (6 Points)

d) (★) Let (X, \preceq) be a poset. Let \prec be the relation on X defined as follows:

$$a \prec b \iff a \preceq b \wedge a \neq b.$$

Prove or disprove that \prec is transitive.

(6 Points)



(★ ★) Let X be a set and let ρ be a countable relation on X . **Prove or disprove** that the transitive closure ρ^* of ρ is countable. (9 Points)



Task 2. Number Theory 17 Points

a) **Short Questions.** Each correct answer gives 1 point. No justification is required. (4 Points)

1.) Compute $R_{13}(2^{4536})$.

2.) Find distinct $k, \ell, m \in \mathbb{N}$ such that $\varphi(k) = \varphi(\ell) = \varphi(m)$, where φ denotes Euler's function.

3.) Compute $\gcd(81, 48 + 3^{25})$.

4.) Compute the multiplicative inverse of 13 modulo 17.

b) (*) Compute the set of solutions $(x, y) \in \mathbb{Z}_{11} \times \mathbb{Z}_{11}$ to the congruence system

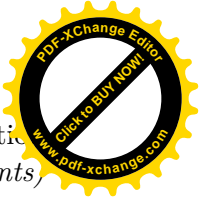
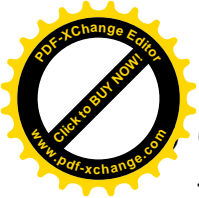
$$2x + 9y \equiv_{11} 7$$

$$2x + 7y \equiv_{11} 5$$

$$4x + 5y \equiv_{11} 1.$$

Show your work.

(4 Points)



(★) Consider the polynomial $f(x) = x^4 + x^2 + 1$. **Prove** that: for all primes $p \in \mathbb{Z}$, the evaluation $f(p)$ is **not** prime. (4 Points)

d) (★ ★) Let φ denote the Euler's function. **Prove or disprove** that for all $n \in \mathbb{N} \setminus \{0\}$ the equation $\varphi(x) = n$ has finetely many solutions $x \in \mathbb{N}$. (5 Points)

Task 3. Algebra 33 Points

a) **Short Questions.** Each correct answer gives the number of points indicated in the brackets. No justification is required.

- 1.) Give the number of subgroups of $\langle \mathbb{Z}_2 \times \mathbb{Z}_6; \oplus \rangle$. (1 Point)

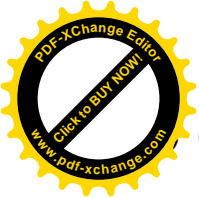
- 2.) Find a generator of a largest cyclic subgroup of $\langle \mathbb{Z}_9^* \times \mathbb{Z}_5^*; * \rangle$ and compute its order, where $(a, b) * (c, d) = (a \odot_9 c, b \odot_5 d)$ for $(a, b), (c, d) \in \mathbb{Z}_9^* \times \mathbb{Z}_5^*$. (2 Points)

- 3.) Compute $R_{x^2+x+1}(x^4 + x^2)$ in $\mathbb{Z}_5[x]$. (2 Points)

- 4.) Find the smallest integer $n > 8$ such that \mathbb{Z}_n^* is isomorphic to \mathbb{Z}_8^* . (2 Points)

- 5.) Compute $\gcd(x^3 + x^2 + x + 1, 2x^3 + x + 3)$ in $\mathbb{Z}_5[x]$. (2 Points)

- b) (*) Let $\langle G; *, \wedge, e \rangle$ be a group and $Z(G) := \{h \mid h \in G, g * h * \hat{g} = h \text{ for all } g \in G\}$ the so-called center of G . **Prove** that $Z(G) = G$ if and only if G is commutative. (5 Points)



(★) Let $\langle R; +, *, -, {}^{-1}, 0, 1 \rangle$ be a commutative ring. **Prove** that the following are equivalent:

- R is an integral domain.
- For all $p(x)$ and $q(x)$ in $R[x]$ it holds that $\deg(p(x) \cdot q(x)) = \deg(p(x)) + \deg(q(x))$.

(4 Points)

d) (★) Let F be a finite field. **Prove** that there exist infinitely many irreducible polynomials in $F[x]$.
(6 Points)



(★ ★) Let $\langle G; \star, \hat{}, e \rangle$ be an abelian group, $k \in \mathbb{N}$ and $H := \{x \mid x \in G, \text{ord}(x) = k\} \cup \{e\}$. **Prove** that H is a subgroup of G if and only if $H = \{e\}$ or k is prime. (9 Points)

Task 4. Logic.....33 Points

a) **Short Questions.** Each correct answer gives the number of points indicated in the brackets. No justification is required.

1.) Circle all *symbols* that occur free in the formula (2 Points)

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

2.) Circle all the formulas in CNF and cross all formulas in DNF in the list below. (2 Points)

$$A \wedge B \wedge \neg C$$

$$A \wedge \neg(B \vee C)$$

$$A \vee (\neg B \wedge C)$$

$$A \vee \neg B \vee \neg C$$

3.) Let $F = \forall x P(x)$. Circle *all* formulas G in the following list such that $F \models G$. (2 Points)

$$\forall x Q(x)$$

$$P(y)$$

$$Q(y) \rightarrow P(z)$$

$$\exists y Q(y)$$

$$(Q(z) \rightarrow Q(y)) \vee (Q(y) \rightarrow Q(z))$$

4.) Find a formula in prenex normal form equivalent to (3 Points)

$$\exists x \left(P(y) \wedge \neg \left(\forall y (Q(x, y) \wedge \exists z R(z, y)) \right) \right).$$

b) (★) **Disprove** that the resolution calculus is complete, that is disprove that for all sets of clauses \mathcal{K} and for all clauses K it holds that

$$\mathcal{K} \models K \implies \mathcal{K} \vdash_{\text{Res}} K.$$

(3 Points)



(★) We extend the resolution calculus with two new rules **ext** and **tnd**. The rules work as follows for all clauses K and all literals L :

$$\begin{aligned} K &\vdash_{\text{ext}} K \cup \{L\}, \\ &\vdash_{\text{tnd}} \{L, \overline{L}\}, \end{aligned} \tag{1}$$

where

$$\overline{L} = \begin{cases} \neg A & \text{if } L = A \text{ for some atomic formula } A, \\ A & \text{if } L = \neg A \text{ for some atomic formula } A. \end{cases}$$

Prove that the rules **ext** and **tnd** are correct.

(3 Points)

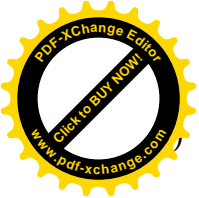


(★ ★ ★) **Prove** that the extended calculus $\text{ResExt} = \{\text{ext}, \text{res}, \text{tnl}\}$ is complete, that is, for all clause sets \mathcal{K} and all clauses K it holds that:

$$\mathcal{K} \models K \implies \mathcal{K} \vdash_{\text{ResExt}} K.$$

Hint: What is the clause set corresponding to the negation of K ?

(11 Points)

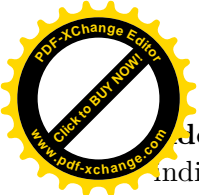


(★ ★) Consider the formulas

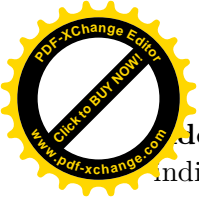
- $F = \forall x \exists y Q(x, y),$
- $G = \forall x Q(x, f(x)).$

Prove or disprove that if F is satisfiable then G is satisfiable.

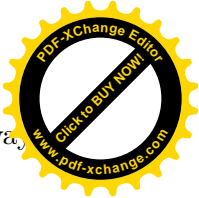
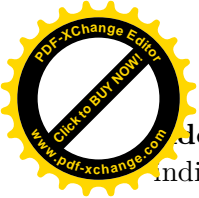
(7 Points)



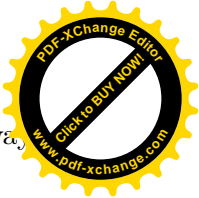
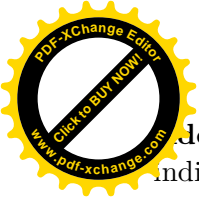
Additional page: Use this sheet in case the space on the exercise sheets is not sufficient. Always indicate the number of the exercise you solve (for example, “Task 3 b”).



Additional page: Use this sheet in case the space on the exercise sheets is not sufficient. Always indicate the number of the exercise you solve (for example, “Task 3 b”).



Additional page: Use this sheet in case the space on the exercise sheets is not sufficient. Always indicate the number of the exercise you solve (for example, “Task 3 b”).



Additional page: Use this sheet in case the space on the exercise sheets is not sufficient. Always indicate the number of the exercise you solve (for example, “Task 3 b”).