Aufgabe 1 (33 Punkte)

Die Aufgaben zum Thema Kryptologie finden Sie auf einem separaten Aufgabenblatt.

Aufgabe 2 (18 Punkte)

Kreuzen Sie in den folgenden Multiple Choice Aufgaben **maximal** je 3 Antworten als richtig an. Tipp: Nehmen Sie sich für das Lesen und Verstehen der Aufgabenstellung viel Zeit, ansonsten verlieren Sie unnötig viele Punkte.

Bewertungshinweis:

- Wenn Sie mehr als drei Kreuze pro Frage ankreuzen, erhalten Sie keine Punkte.
- Haben Sie alle richtigen Antworten angekreuzt, erhalten Sie die volle Punktzahl.
- Haben Sie eine richtige Antwort zu wenig angekreuzt, erhalten Sie die halbe Punktzahl.
- Ansonsten erhalten Sie keine Punkte.

(2.1) (3 Punkte) Seien $R_1 \subseteq M_1 \times M_2$, $R_2 \subseteq M_2 \times M_3$ und $R_3 \subseteq M_3 \times M_4$ beliebige Relationen

und $I = \{(x,x) | x \in M\}$.

Es gilt:

❑ $R_1 \circ R_1^{-1} = R_1^{-1} \circ R_1 = I$.

❑ R^{-1} ist nur definiert, wenn $R \neq \emptyset$.

✓ $(R_1^{-1})^{-1} = R_1$.

✓ $(R_1 \circ R_2) \circ R_3 = R_1 \circ (R_2 \circ R_3)$

✓ $(R_1 \circ R_2)^{-1} = R_2^{-1} \circ R_1^{-1}$.

❑ $(R_1 \circ R_2)^{-1} = R_1^{-1} \circ R_2^{-1}$.

❑ $R_1 \circ R_2 = R_2 \circ R_1$.

(2.2) (3Punkte) Sei M eine nichtleere Menge und $R, S \subseteq M \times M$ eine beliebige Relation.

✓ Wenn R irreflexiv ist, ist R^{-1} auch irreflexiv.

❑ Wenn R nicht irreflexiv ist, ist R reflexiv.

✓ Wenn R asymmetrisch ist, so ist R antisymmetrisch.

❑ Wenn R symmetrisch und transitiv ist, so ist R auch reflexiv.

✓ Wenn R und S symmetrisch sind, dann ist auch $R \cup S$ symmetrisch.

❑ Wenn R und S transitiv sind, dann ist auch $R \cup S$ transitiv.

(2.3) (3 Punkte) Sei M eine beliebige nichtleere Menge und $A \subseteq M$ eine beliebige Teilmenge. Sei $\sqsubseteq$ eine beliebige Ordnungsrelation in M.

❑ Wenn A nichtleer ist, dann hat A ein größtes Element.

❑ Wenn A nichtleer ist, dann hat A ein maximales Element.

✓ Wenn $a \in M$ ein beliebiges Element ist, dann hat die Menge [?…?] Schranken von {a} das größte Element a .

✓ Wenn $M = \mathbb{N}_0$ und die Ordnungsrelation die Teilbarkeit ist [?existiert?] das größte Element von M.

❑ Wenn A eine obere Schranke hat, dann ist A nicht leer.

✓ Wenn A leer ist, dann ist jedes Element von M untere Schranke.

(2.4) (3 Punkte) Sei *M* eine beliebige nichtleere Menge und $A \subseteq M$ eine beliebige Teilmenge. Sei $\equiv$ eine beliebige Äquivalenzrelation in *M*.

❑ Wenn $x \in M$ verschieden von $y \in M$ ist, dann sind die Äquivalenzklassen von x und y elementfremd.

✓ Wenn die Äquivalenzklassen von $x \in M$ und $y \in M$ verschieden sind, dann sind x und y verschieden.

❑ Wenn die Äquivalenzklassen von $x \in M$ und $y \in M$ gleich sind, dann sind x und y gleich.

✓ Wenn zwei Äquivalenzklassen ein gemeinsames Element haben sind sie gleich.

❑ Jede Äquivalenzklasse hat einen eindeutig festgelegten Repräsentanten.

✓ Äquivalenzklassen sind immer nichtleer.

(2.5) (3 Punkte) Seien $R_1 : M_1 \to M_2$ und $R_2 : M_2 \to M_3$ beliebige Abbildungen.

Dafür, dass $R_1 \circ R_2$ surjektiv ist,

¬❑ ist hinreichend, dass R_2 surjektiv ist.

✓ ist notwendig, dass R_2 surjektiv ist.

❑ ist hinreichend, dass R_1 surjektiv ist.

❑ ist notwendig, dass R_1 surjektiv ist.

¬❑ ist notwendig, dass R_1 oder R_2 surjektiv ist.

❑ ist hinreichend, dass R_1 und R_2 surjektiv sind.

¬❑ ist notwendig, dass R_1 injektiv ist.

¬❑ ist hinreichend, dass R_1 surjektiv und R_2 injektiv sind.

❑ ist notwendig und hinreichend, dass R_1 und R_2 surjektiv sind.

✓ ist weder notwendig noch hinreichend, dass R1 surjektiv ist.

(2.6) (3 Punkte) Sei $(G, \circ)$ eine Gruppe.

Welche der folgenden Aussagen ist richtig?

✓ Die Gleichung $a \circ x = b$ ist für beliebige $a \in G$ und $b \in G$ immer durch ein $x \in G$ lösbar.

✓ Die Gleichung $x \circ a = b$ ist für beliebige $a \in G$ und $b \in G$ immer durch ein $x \in G$ lösbar. Diese Lösung ist eindeutig.

❑ Die Gleichungen $a \circ x = b$ und $x \circ a = b$ sind für beliebige $a \in G$ und $b \in G$ immer durch ein $x \in G$ lösbar. Diese Lösung ist eindeutig.

✓ Es gibt genau ein $e \in G$, so dass für alle $a \in G$ gilt: $a \circ e = e \circ a = a$.

❑ Es gibt genau ein $e \in G$, so dass für alle $a \in G$ gilt: $a \circ e = e \circ a = e$.

❑ Es gibt genau ein $a' \in G$, so dass für alle $a \in G$ gilt: $a \circ a' = a' \circ a = e$.

Aufgabe 3 (9 Punkte)

Sei $M = \{a,b,c\}$. Geben Sie ein Beispiel für eine Relation $R \subseteq M \times M$ an, die

(3.1) (3 Punkte) irreflexiv, symmetrisch aber nicht transitiv ist.

(3.2) (3 Punkte) reflexiv, antisymmetrisch und transitiv ist.

(3.3) (3 Punkte) antisymmetrisch aber nicht asymmetrisch und nicht symmetrisch ist.

Aufgabe 4 (21 Punkte)

Sei $M = \mathbb{R}$ die Menge aller reellen Zahlen. Die Relation $\equiv$ sei durch

$$x \equiv y \Leftrightarrow x^2 = y^2$$

definiert. $x \equiv y$ heißt nichts anderes, als dass x und y denselben Betrag haben.

(4.1) (3 Punkte) Geben Sie die formale Definition einer Äquivalenzrelation $\equiv \subseteq M \times M$. (Mit Quantoren, nur Eigenschaften aufzählen reicht nicht!)

(4.2) (6 Punkte) Beweisen Sie, dass es sich bei $\equiv$ um eine Äquivalenzrelation handelt.

(4.3) (2 Punkte) Geben Sie die Äquivalenzklassen von 1 und 0 an.

(4.4) (10 Punkte) Beweisen Sie oder widerlegen Sie, dass die durch $[x]_= \oplus [y]_= = [x+y]$ definierte Addition bzw. das durch $[x]_= \odot [y]_= = [x \cdot y]$ definierte Produkt unabhängig vom Repräsentanten ist.

Aufgabe 5 (19 Punkte)

Rechnen in Restklassenstrukturen

(5.1) (2 Punkte) Dass eine Aufgabe nicht eindeutig lösbar ist, kann zwei Gründe haben. Welche sind das? Bitte antworten Sie mit zwei deutschen Sätzen.

____

____

(5.2) (6 Punkte) Welche der folgenden Aufgaben ist eindeutig lösbar? Schreiben Sie „eindeutig lösbar“ / „nicht eindeutig lösbar“ hinter die Aufgabe.

1. $[16]_{64} \cdot [x]_{64} = [8]_{64}$ nicht eindeutig lösbar
2. $[17]_{64} \cdot [x]_{64} = [16]_{64}$ eindeutig lösbar
3. $[18]_{64} \cdot [x]_{64} = [32]_{64}$ nicht eindeutig lösbar

(5.3) (11 Punkte) Berechnen Sie die Lösung der Gleichung $[207]_{5814} \cdot [x]_{5814} = [45]_{5814}$