Aufgabe 1 (33 Punkte)

Der Klausurteil von Herrn Neuhaus wird auf einem separatem Aufgabenblatt ausgeteilt.

Aufgabe 2 (18 Punkte)

Kreuzen Sie in den folgenden Multiple Choice Aufgaben **maximal** je 3 Antworten als richtig an.

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 $R \neq \emptyset$.
- ❑ $(R_1^{-1})^{-1} = R_1$.
- ❑ $(R_1 \circ R_2)^{-1} = R_1^{-1} \circ R_2^{-1}$.
- ❑ $(R_1 \circ R_2)^{-1} = R_2^{-1} \circ R_1^{-1}$.
- ❑ $R_1 \circ R_2 = R_2 \circ R_1$.
- ❑ $(R_1 \circ R_2) \circ R_3 = R_1 \circ (R_2 \circ R_3)$

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

- ❑ Wenn R nicht irreflexiv ist, ist R reflexiv.
- ❑ Wenn R irreflexiv ist, ist R nicht reflexiv.
- ❑ Wenn R symmetrisch und transitiv ist, so ist R auch reflexiv.
- ❑ Wenn R asymmetrisch ist, so ist R irreflexiv.
- ❑ 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 zwei verschiedene maximale Elemente hat, dann hat A kein größtes Element.
- ❑ Wenn A ein größtes Element hat, dann ist A nicht leer.
- ❑ Wenn A eine obere Schranke hat, dann ist A nicht leer.
- ❑ Wenn A leer ist, dann ist jedes Element von M obere Schranke.

(2.4) (3 Punkte) Sei *M* eine beliebige nichtleere Menge und A ⊆ M eine beliebige Teilmenge. Sei ≡ eine beliebige Äquivalenzrelation in *M*.

- ❑ Wenn x ∈ *M* verschieden von y ∈ *M* ist, dann sind die Äquivalenzklassen von x und y elementfremd.
- ❑ Wenn die Äquivalenzklassen von x ∈ *M* und y ∈ *M* verschieden sind, dann sind x und y verschieden.
- ❑ Wenn die Äquivalenzklassen von x ∈ *M* und y ∈ *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 $R_1 \circ R_2$ injektiv ist,

- ❑ ist hinreichend, dass R_1 injektiv ist.
- ❑ ist notwendig, dass R_1 injektiv ist.
- ❑ ist hinreichend, dass R_2 injektiv ist.
- ❑ ist notwendig, dass R_2 injektiv ist.
- ❑ ist hinreichend, dass R_1 und R_2 injektiv sind.
- ❑ ist notwendig, dass R_1 und R_2 injektiv sind.
- ❑ ist hinreichend, dass R_1 oder R_2 injektiv ist.
- ❑ ist notwendig, dass R_1 oder R_2 injektiv ist.
- ❑ ist weder notwendig noch hinreichend, dass R_1 injektiv ist.
- ❑ ist weder notwendig noch hinreichend, dass R_2 injektiv ist.

(2.6) (3 Punkte) Sei (G, ∘) eine Gruppe.

Welche der folgenden Aussagen ist richtig?

- ❑ 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: $a \circ a' = a' \circ a = e$.
- ❑ 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. Die 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.

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) reflexiv, symmetrisch aber nicht transitiv ist.

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

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

Aufgabe 4 (21 Punkte)

Sei $M = \mathbb{R} \times \mathbb{R}$ die Menge alle Punkte in der x,y Ebene. Die Relation $\equiv$ sei durch

$$(x,y) \equiv (u,v) \Leftrightarrow x^2 + y^2 = u^2 + v^2$$

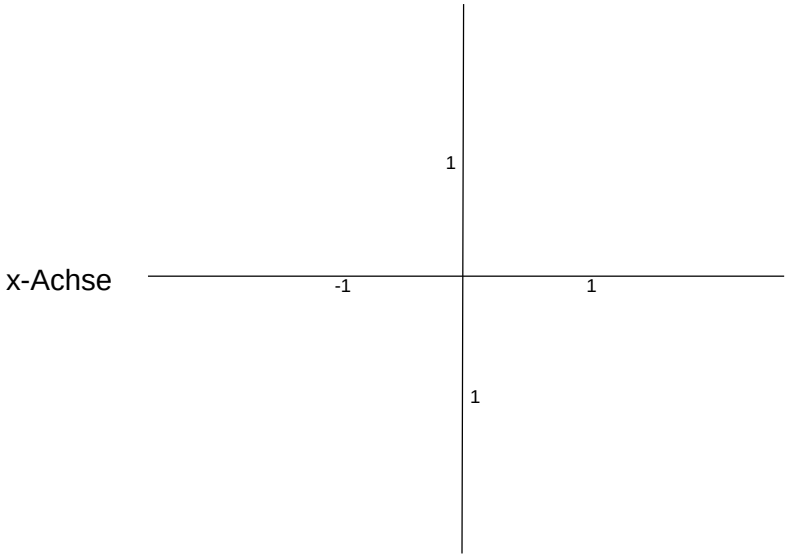
Definiert. Hinweis zum besseren Vorstellen: Da $x^2 + y^2$ das Quadrat des Abstandes des Punktes (x,y) vom Ursprung angibt, bedeutet $(x,y) \equiv (u,v)$, dass die Punkte (x,y) und (u,v) denselben Abstand vom Ursprung haben. Das heißt nichts anderes, als dass sie auf demselben Kreis um den Ursprung liegen.

(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.

Tipp: Bitte berücksichtigen Sie, dass es sich bei den Elementen der Menge M um Paare handelt.

(4.3) (4 Punkte) Skizzieren Sie die Äquivalenzklasse des Punktes (-1,1) in der x,y Ebene und geben Sie die Koordinaten von drei weiteren Punkten dieser Äquivalenzklasse an.



(4.4) (8 Punkte) Beweisen Sie, dass das durch $(x,y) \odot (u,v) = (x \cdot u - y \cdot v, x \cdot v + y \cdot u)$ definierte Produkte von zwei Punkten unabhängig vom Repräsentanten ist.

Tipp: Beweisen Sie mit Hilfe der ersten und zweiten binomischen Formeln

$$(x \cdot u - y \cdot v)^2 + (x \cdot v + y \cdot u)^2 = (x^2 + y^2) \cdot (u^2 + v^2)$$

Anschaulich bedeutet diese Formel, dass der Abstand des Produktes vom Nullpunkt gleich dem Produkt der Abstände vom nullpunkt ist. Danach brauchen Sie nur noch hin zu schreiben, was die „Unabhängigkeit vom Repräsentanten“ bedeutet.

Aufgabe 5 (20 Punkte)

Rechnen in Restklassenstrukturen

(5.1) (6 Punkte) Welche der folgenden Aufgaben ist eindeutig lösbar? Schreiben Sie „eindeutig lösbar“ / „nicht eindeutig lösbar“ hinter die Aufgabe.

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

(5.2) (14 Punkte) Berechnen Sie alle Lösungen der Gleichung $[207]_{5814} \cdot [x]_{5814} = [45]_{5814}$

Aufgabe B1 (9 Punkte):

Geben Sie an, ob folgende Aussagen wahr oder falsch sind. (Hinweis: Inkorrekte Antworten führen nicht zu Abzügen. Punkte werden ab 10 korrekten Antworten vergeben):

Aussage	*Wahrheitswert*
1. Eine Verschlüsselungsfunktion muss injektiv (linkseindeutig) sein.	
2. Bei symmetrischen Verschlüsselungsverfahren sind die Ver- und Entschlüsselungsfunktionen identisch.	
3. Bei asymmetrischen Verschlüsselungsverfahren ist der private Schlüssel prinzipiell nicht aus dem öffentlichen Schlüssel berechenbar.	
4. Bei asymmetrischen Verschlüsselungsverfahren kann der Sender die von ihm verschlüsselte Nachricht nicht wieder entschlüsseln.	
5. Das Schutzziel „Authentizität“ bedeutet, dass eine Nachricht nicht unbemerkt verändert werden kann.	
6. Das Kerckhoffs´sche Prinzip besagt, dass die verwendeten Verschlüsselungsverfahren geheim gehalten werden müssen.	
7. Bei asymmetrischen Verschlüsselungsverfahren können immer Chosen-Plaintext-Angriffe durchgeführt werden.	
8. Die Skytale-Verschlüsselung ist eine Permutations-Chiffre.	
9. Permutations-Chiffren sind auch bei einer sehr großen Schlüsselmenge anfällig gegenüber Häufigkeitsanalysen.	
10. Bei polyalphabetischen Substitutionsverfahren wird für den verschlüsselten Text ein anderes Alphabet verwendet als für den Klartext.	
11. Ein Kryptosystem ist perfekt sicher, wenn für beliebige Klar- und Geheimtexte einer gegebenen Länge die a priori Wahrscheinlichkeit größer als die a posteriori Wahrscheinlichkeit ist.	
12. Das One-Time-Pad gilt als sicher, weil es sich nur mit extrem hohem Rechenaufwand brechen lässt.	
13. Die Euler´sche Phi-Funktion liefert die Anzahl der zu n teilerfremden natürlichen Zahlen zwischen 1 und n.	
14. Ein Nachteil von asymmetrischen gegenüber symmetrischen Verschlüsselungsverfahren ist, dass jeder Teilnehmer zwei Schlüssel benötigt.	
15. Das RSA-Verfahren ist sicher, weil große Potenzen modulo n nicht mit vertretbarem Aufwand berechnet werden können.	
16. Eine Carmichael-Zahl ist keine echte Primzahl.	
17. Falls der Fermat-Text zurückliefert, dass eine gegebene Zahl keine Primzahl ist, so kann man sich darauf 100%-ig verlassen.	
18. Durch den Baby-Step-Giant-Step-Algorithmuss kann der diskrete Logarithmus auch bei extrem großen Werten in vertretbarer Zeit ermittelt werden.	

Aufgabe B2 (8 Punkte):

Der Geheimtext NEIREF wurde abgefangen. Welcher der drei Wörter „safran“, „reifen“ und „basalt“ könnte der zugrundeliegende Klartext sein, wenn

a) eine Transpositions-Chiffre,

b) eine Caesar-Verschlüsselung,

c) eine Pemutations-Chiffre,

d) eine Vigenère-Verschlüsselung mit einer Schlüssellänge 3 bzw. 5,

e) ein One-Time-Pad

verwendet wurde? Begründen Sie Ihre Antwort.

Aufgabe B3 (8 Punkte):

Für das RSA-Verfahren werden folgende Werte gewählt: p=11, q=17 und e=21.

a) Ermitteln Sie den öffentlichen und privaten Schlüssel. Geben Sie die Zwischenschritte Ihrer Berechnung an.
b) Verschlüsseln Sie die Nachricht m=5. Erläutern Sie Ihren Rechenweg.

Aufgabe B4 (4 Punkte):

Prüfen Sie mithilfe des Miller-Rabin-Text, ob 121 eine Primzahl ist. Wählen Sie als Basis a=3. Notieren Sie alle Zwischenschritte. Was wissen Sie nach dem Test über 121?

Aufgabe B5 (4 Punkte):

Alice und Bob führen das Diffie-Hellman-Verfahren durch. Sie einigen sich dazu öffentlich auf die Primzahl p=11 und das erzeugende Element g=2. Alice wählt eine geheime Zahl a=4 und berechnet

$x=g^a \bmod p=2^4 \bmod 11=5$. Alice schickt x an Bob und erhält von ihm im Gegenzug y=3. Welche geheime Zahl b hat Bob gewählt? Welchen Wert hat der gemeinsame private Schlüssel von Alice und Bob? Geben Sie Ihren Rechenweg an.