Ist der Raum $\langle v_1, v_2 \rangle$ (orthogonales) Komplement von $\langle v_3 \rangle$:

$v_1 = \begin{pmatrix} 1 \\ -4 \\ 3 \end{pmatrix}$, $v_2 = \begin{pmatrix} 2 \\ 0 \\ 2 \end{pmatrix}$, und $v_3 = \begin{pmatrix} -2 \\ 1 \\ 2 \end{pmatrix}$

Die richtige Antwort ist: Orthogonales Komplement

Welche der folgenden Aussagen sind allgemein g{ü}ltig (d.h. f{ü}r beliebige mathematische Aussagen φ, ψ)
Zur Erinnerung: $\varphi \to \psi$ hei{ß}t "wenn dann" bzw "impliziert"; $\leftrightarrow$ hei{ß}t "gdw" oder "{ä}quivalent", $\wedge$ hei{ß}t "und", $\vee$ "oder" und $\neg$ "nicht".

Die richtigen Antworten sind: $\neg\psi \to \big((\varphi \to \psi) \leftrightarrow \neg\varphi\big)$.
, $(\varphi \to \neg\varphi) \vee (\neg\varphi \to \varphi)$

F{ü}r welche H, G ist G Untergruppe von H?

Die richtigen Antworten sind: $H = \mathrm{GL}(2)$ (mit Matrixmultiplikation) und G die Diagonalmatrizen in $\mathrm{GL}(2)$.
, $H = (V, +)$ f{ü}r V der Vektorraum $\mathbb{R}^2$, und $G = \left\{ \begin{pmatrix} x \\ -x \end{pmatrix} : x \in \mathbb{R} \right\}$

Welcher der folgenden S{ä}tze gilt allgemein für reelle $n \times n$ Matrizen A:

Die richtigen Antworten sind: Wenn λ Eigenwert von A ist, dann ist λ^2 Eigenwert von A^2.
, Zwei Eigenvektoren zu verschiedenen Eigenwerten sind linear unabhängig.

Der {ö}ffentliche RSA Schl{ü}ssel $(e, n) = (27, 55)$ ist gegeben. Brechen Sie die Verschl{ü}sselung mit brute force, d.h. berechnen Sie den private key (d, n). Als Antwort geben Sie d an.

Die richtige Antwort ist: 3

F{ü}r welche der folgenden Gruppen G, H t{ä}{ß}t sich G in H einbetten? (Mit Einbettung bezeichnen wir einen injektiven Homomorphismus.)
($\mathrm{GL}(n)$ sind die invertierbaren $n \times n$-Matrizen {ü}ber einem K{ö}rper K, mit der Matrix-Multiplikation als Verkn{ü}pfung.)

Die richtigen Antworten sind: $G = (K, +)$ und H die $n \times n$ Matrizen {ü}ber K mit der Matrix-Addition (wobei K ein beliebiger K{ö}rper ist).
, $G = (\mathbb{Z}_2, +)$ und $H = (\mathbb{Z}_6, +)$

F{ü}r welche der gegebenen G, n hat die Gruppe G hat eine Untergruppe der Gr{ö}{ß}e n?

Die richtigen Antworten sind: $G = S_4$, $n = 12$
, $G = (\mathbb{Z}_{30}, +)$, $n = 5$

Welche Aussagen bzw Gleichungen gelten in allen Gruppen $(G, \circ)$:

Die richtige Antwort ist: $(a \circ b \circ c \circ d)^{-1} = (c \circ d)^{-1} \circ (a \circ b)^{-1}$

Welche der folgenden Aussagen sind allgemein g{ü}ltig, d.h. f{ü}r beliebige mathematische Aussagen φ, ψ, und f{ü}r eine beliebige (m{ö}glicherweise leere) Menge A.
Zur Erinnerung: $\varphi \to \psi$ hei{ß}t "wenn dann" bzw "impliziert"; $\leftrightarrow$ hei{ß}t "gdw" oder "{ä}quivalent", $\wedge$ hei{ß}t "und", $\vee$ "oder" und $\neg$ "nicht", $\exists$ hei{ß}t 'es gibt" und $\forall$ hei{ß}t 'f{ü}r alle".

Die richtigen Antworten sind: $(A \neq \emptyset$ und $\forall x \in A\ \varphi(x))$ impliziert $\exists x \in A\ \varphi(x)$
, $\neg(\exists x \in A) \neg\varphi(x)$ gdw $(\forall x \in A)\varphi(x)$

Welche der folgenden Abbildungen ist immer bijektiv:

Die richtigen Antworten sind: $f : G \to G$ $a \mapsto a \circ b$ f{ü}r eine Gruppen G und $b \in G$.
, $f : V \to V$ $v \mapsto \lambda v$ für einen Vektorraum V über K und $\lambda \neq 0$ in K.

Sei B {ä}hnlich zu A, d.h. $B = U^{-1}AU$ f{ü}r ein $U \in \mathrm{GL}(n)$. Was gilt allgemein:

Die richtigen Antworten sind: $A = I$ (die Identit{ä}tsmatrix) gdw $B = I$
, $\mathrm{Tr}(A) = \mathrm{Tr}(B)$ (Spur)

Ist das folgende Beweisprinzipien g{ü}ltig: $\varphi(x)$ gilt f{ü}r alle $x \in A := \{n \in \mathbb{Z} : n \geq -2\}$, wenn gilt: $\varphi(-2)$, und f{ü}r alle $n \in A$ gilt: $\varphi(n) \to \varphi(n+1)$.

Die richtige Antwort ist: Ja

Welche der folgende Anssagen gilt allgemein:

Die richtigen Antworten sind: Eine Vektorraum-Einbettung (inj. lineare Abbildung) $f : V \to V$, f{ü}r einen endlich-dimensionalen Vektorraum f, ist immer bijektiv.
, Die Verkn{ü}pfung $g \circ f$ einer injektiven Funktion f mit einer bijektiven Funktion g ist injektiv.

Gegeben der public key (n, e). Der dazugehörige private key ist (n, d), mit $n = pq$, wobei p, q so große Primzahlen sind dass man n de facto nicht ohne zusätzliche Information faktorisieren kann. Sei c_1 der verschlüsselte Ciphertext zum Klartext t_1, und c_2 der verschlüsselte Ciphertext zu einem anderen Klartext t_2. Welche der folgenden Informationen reichen aus um den Schlüssel (effizient) zu knacken?

Die richtigen Antworten sind: q
, $\varphi(n)$

Welcher der folgenden S{ä}tze gilt f{ü}r alle $n \times n$ Matrizen (bzw f{ü}r alle invertierbaren $n \times n$-Matrizen, falls A^{-1} erw{ä}hnt wird):

Die richtigen Antworten sind: Wenn $A = A^{-1}$, dann ist $\det(A)^2 = 1$
, Wenn A Projektion ist, dann ist $\mathrm{Tr}(A)$ ganzzahlig.

Welche der folgenden Zahlen sind Eigenwerte der Matrix A? (Wenn A keine Eigenwerte hat ist keine Zahl anzukreuzen, wenn A genau einen EW hat dann ist dieser EW anzukreuzen, wenn A zwei verschiedene hat dann sind beide, etc.
$A = \begin{pmatrix} -4 & 2 \\ -2 & 2 \end{pmatrix}$

Die richtigen Antworten sind: $-\sqrt{5} - 1$
, $-1 + \sqrt{5}$

F{ü}r $G = (\mathbb{Z}_{12}, +)$, $U = \langle \bar{6} \rangle$, $a = \bar{2}$. Wieviele Elemente hat die Linksnebenklasse aU?

Die richtige Antwort ist: 2

Welche der folgenden Strukturen ist eine Gruppe?

Die richtigen Antworten sind: $\{q \in \mathbb{Q} : q > 0\}, \cdot)$
, $(L(n), +)$, die $n \times n$-Matrizen mit der Matrixaddition.

Sei E die Standardbasis. Gegeben die Orthonormalbasis $B = (b_1, b_2, b_3)$ und f die lineare Funktion mit E-Darstellung A. Sei C die B-Darstellung von f. Gib $c_{1,1}$ an (d.h. den Eintrag in der ersten Zeile und ersten Spalte von C).
$b_1 = \begin{pmatrix} \frac{1}{3} \\ -\frac{2}{3} \\ \frac{2}{3} \end{pmatrix}$, $b_2 = \begin{pmatrix} \frac{2}{3} \\ \frac{2}{3} \\ \frac{1}{3} \end{pmatrix}$, $b_3 = \begin{pmatrix} -\frac{2}{3} \\ \frac{1}{3} \\ \frac{2}{3} \end{pmatrix}$ und $A = \begin{pmatrix} 1 & 1 & 2 \\ 2 & 1 & 2 \\ 0 & 1 & 2 \end{pmatrix}$

Die richtige Antwort ist: $-\frac{1}{9}$

Berechne (z.B. mithilfe des Euklidischen Algorithmus) $\bar{b} = \bar{a}^{-1}$ in $\mathbb{Z}_n$.
Genauer: Finde $0 \leq b < n$ s.d $\bar{a} \cdot \bar{b} = 1$ in $\mathbb{Z}_n$, oder {ä}quivalent: $a \cdot b \equiv 1 \mod n$.
Als Antwort ist nicht b gefragt, sondern $b \mod 5$, d.h. das $0 \leq c < 5$ mit $b \equiv c \mod 5$.
(Bsp: Angenommen $n = 9$ und $a = 2$, dann ist $b = 5$ (weil $2 \cdot 5 = 10 \equiv 1 \mod 9$; die Antwort ist dann $c = 0$, weil $5 \equiv 0 \mod 5$.)
Geben Sie dieses c an f{ü}r: $a = 25$ und $n = 42$.

Die richtige Antwort ist: 2

Ist die folgende Teilmenge 2×2 Matrizen {ü}ber $\mathbb{R}$ unter (Matrizen)multiplikation abgeschlossen? Ein Ring? Ein Unterring der 2×2 Matrizen? (Ringe müssen ein Einselement enthalten, Unterringe darüber hinaus dasselbe Einselement wie der Ring.)

Die Matrizen der Form $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$ f{ü}r $a \in \mathbb{R}$

Die richtige Antwort ist: Ring aber kein Unterring.

Die Vektoren $v_1 = \begin{pmatrix} 1 \\ 2 \\ -2 \end{pmatrix}$, $v_2 = \begin{pmatrix} 0 \\ 1 \\ 2 \end{pmatrix}$ und $v_3 = \begin{pmatrix} 2 \\ 1 \\ 0 \end{pmatrix}$ lassen sich durch "modulo Rechnen" über jedem Grundkörper $\mathbb{Z}_p$ interpretieren. So ist z.B. v_1 in $\mathbb{Z}_2$ gleich $\begin{pmatrix} \bar{1} \\ \bar{0} \\ \bar{0} \end{pmatrix}$. Für welche p gilt, dass $\{v_1, v_2, v_3\}$ l.u. in $\mathbb{Z}_p^3$ ist?

Die richtigen Antworten sind: 3, 7, 11

Ist die Folgende Menge ein Unterring der 7×7 Matrizen {ü}ber $\mathbb{R}$? (Unterringe m{ü}ssen per Definition dasselbe Einselement enthalten.)
Die unteren Dreiecksmatrizen, d.h. $a_{i,j} = 0$ wenn $i < j$.

Die richtige Antwort ist: Ja

H sei die Menge der ungeraden Permutationen der S_4. Was gilt:

Die richtige Antwort ist: $|H| = 12$

Wenn B durch eine elementare Zeilenoperation aus A konstruieren kann, dann ist B {ä}hnlich zu A (dh. $B = T^{-1}AT$ f{ü}r ein $T \in \mathrm{GL}(n)$.)

Die richtige Antwort ist: Nein

Sei G eine Gruppe. Welche der folgenden Sätze gilt allgemein:

Die richtigen Antworten sind: Wenn G endlich ist und 7 die Ordnung von G teilt, dann hat G eine Untergruppe der Größe 7.
, Wenn G endlich ist und U eine Untergruppe, dann teilte die Ordnung von U die Ordnung von G.

Jedes Polynom $f(X) \in \mathbb{Z}_2[X]$ von Grad 2 hat eine Nullstelle in $\mathbb{Z}_2[X]$. (D.h.: Jede Funktion $f : \mathbb{Z}_2 \to \mathbb{Z}_2$ der Form $f(x) = a_2x^2 + a_1x + a_2$, mit $a_i \in \mathbb{Z}_2$ und $a_2 \neq 0$.)

Die richtige Antwort ist: Nein

Bilden die Vektoren x, y eine Orthonormalbasis des $\mathbb{R}^3$, eine Basis aber keine Orthonormalbasis, oder keine Basis? F{ü}r: $x = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $y = \begin{pmatrix} 0 \\ -1 \end{pmatrix}$

Die richtige Antwort ist: Keine Basis

Bilden die Vektoren x, y, z eine Orthonormalbasis des $\mathbb{R}^3$, eine Basis aber keine Orthonormalbasis, oder keine Basis? F{ü}r: $x = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$, $y = \begin{pmatrix} -1 \\ 1 \\ 1 \end{pmatrix}$, $z = \begin{pmatrix} 0 \\ -1 \\ 1 \end{pmatrix}$

Die richtige Antwort ist: Basis aber keine Orthonormalbasis