1. **a)** Setzt man

$$A \;=\; \begin{pmatrix} 2 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 5 \end{pmatrix}$$

so rechnet man sofort nach, daß die drei Einheitsvektoren Eigenvektoren zu diesen drei Eigenwerten sind:

$$A \circ \vec{e}_1 \;=\; 2\vec{e}_1 \quad A \circ \vec{e}_2 \;=\; 3\vec{e}_1 \quad A \circ \vec{e}_3 \;=\; 5\vec{e}_1$$

Da A eine 3×3-Matrix ist, kann A nicht mehr als 3 Eigenwerte besitzen.

b) Setze

$$I \;=\; \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 0 & 0 & 1 \end{pmatrix}$$

Dann ist offenbar $I \neq E$, obwohl I nur den Eigenwert 1 besitzt. Das letztere erkennt man daran, daß das charakteristische Polynom von I

$$\det(I - tE) \;=\; (1-t)^3$$

nur die Nullstelle 1 besitzt.

2. Aufgrund der Angaben gelten für den Übergang vom t-ten zum $t+1$-ten Jahr die Gleichungen

$$\begin{aligned} v_{t+1,1} &= \frac{1}{10} \cdot v_{t,2} + v_{t,3} \\ v_{t+1,2} &= v_{t,1} \\ v_{t+1,3} &= \frac{9}{10} \cdot v_{t,2} \end{aligned}$$

Dieses ergibt die Übergangsmatrix

$$A \;=\; \begin{pmatrix} 0 & \frac{1}{10} & 1 \\ 1 & 0 & 0 \\ 0 & \frac{9}{10} & 0 \end{pmatrix}$$

Eine Fahrzeugverteilung $\vec{v}_*$ ist konstant, wenn sie sich von einem Jahr zum nächsten nicht verändert, d. h. falls gilt

$$A \circ \vec{v}_* \;=\; \vec{v}_*$$

Dieses bedeutet, daß eine mögliche konstante Verteilung durch einen Eigenvektor $\vec{v}_*$ zum Eigenwert 1 dargestellt wird. Falls die Matrix A tatsächlich einen solchen Eigenwert besitzt, muß das homogene Gleichungssystem

$$(A - E) \circ \vec{x} \;=\; \begin{pmatrix} -1 & \frac{1}{10} & 1 \\ 1 & -1 & 0 \\ 0 & \frac{9}{10} & -1 \end{pmatrix} \circ \vec{x} \;=\; 0$$

eine von Null verschiedene Lösung besitzen. Man prüft dieses nach, indem man die Matrix $A - E$ mit dem Gaußschen Verfahren reduziert; man erhält als reduzierte Matrix

$$\begin{pmatrix} 1 & -\frac{1}{10} & -1 \\ 0 & 1 & -\frac{10}{9} \\ 0 & 0 & 0 \end{pmatrix}$$

Man erkennt, daß diese Matrix den Rang 2 bzw. den Corang $1 = 3-2$ und damit eine von Null verschiedene Grundlösung besitzt. Diese Grundlösung und damit ein Eigenvektor der Matrix A zum Eigenwert 1 lautet

$$\vec{u} \;=\; \begin{pmatrix} 10/9 \\ 10/9 \\ 1 \end{pmatrix}$$

Als mögliche konstante Verteilungen kommen positive Vielfache von $\vec{u}$ in Frage:

$$\vec{v}_* \;=\; \mu \cdot \vec{u} \quad \text{mit} \quad \mu > 0$$

Unabhängig vom Faktor μ gilt bei einer solchen konstanten Verteilung: je 34.5% der Fahrzeuge sind ein oder zwei Jahre alt, 31.0% der Fahrzeuge sind drei Jahre alt.

Bemerkung: Man kann natürlich auch mit Hilfe des charakteristischen Polynoms der Matrix A nachprüfen, ob diese Matrix den Eigenwert 1 besitzt. Das charakteristische Polynom lautet:

$$p(t) \;=\; -t^3 + 0.1t + 0.9$$

$p(t)$ besitzt nur die (reelle) Nullstelle 1.

3. Lösung: Aufgrund der Information des Spitzels weiß man, daß der Klartextbuchstabe "R" im Schlüsseltext dem Buchstaben "W" entspricht. Ist k der (zunächst noch unbekannte) Schlüssel, so muß aufgrund der Arbeitsweise des Caesar-Verfahrens gelten:

$$\mathrm{R} + k \;=\; \mathrm{W} \mod 26 \qquad \text{bzw.} \qquad 17 + k \;=\; 22 \mod 26$$

Daher ist lautet der Schlüssel $k = 5$ bzw. $k \hat{=} \mathrm{F}$. Damit kann jetzt der Text entschlüsselt werden:

$$\begin{array}{rl} & \mathrm{INJBJYYJWFZXXNHMYJSXNSISNHMYLZY} \\ - & \mathrm{FFFFFFFFFFFFFFFFFFFFFFFFFFFFF} \\ \hline \end{array}$$

Man ersetzt hier jeden Buchstaben durch seine Nummer aus $\{0, \ldots, 25\}$:

$$\begin{array}{rl} & 8\,13\;9\;\;1\;\;9\,24\,24\;\;9\,22\;\;5\,25\,23\,23\,13\;\;7\,12\,24\;\;9\,18\,23\,13\,18\;\;8\,18\,13\;\;7\,12\,24\,11\,25\,24 \\ - & 5\;\;5\,5\;\;5\,5\;\;5\;\;5\,5\;\;5\,5\;\;5\,5\;\;5\;\;5\,5\;\;5\,5\;\;5\;\;5\,5\;\;5\;\;5\,5\;\;5\;\;5\,5\;\;5\;\;5\,5\;\;5\;\;5\;\;5\;\;5 \\ \hline & 3\;\;8\;4\,22\;4\,19\,19\;4\,17\;\;0\,20\,18\,18\;\;8\;\;2\;\;7\,19\;\;4\,13\,18\;\;8\,13\;\;3\,13\;\;8\;\;2\;\;7\,19\;\;6\,20\,19 \mod 26 \\ \hat{=} & \mathrm{D\;\;I\,E\,W\,E\;\;T\;\;T\,E\;\;R\,A\;\;U\;\;S\;\;S\;\;I\,C\;\;H\;\;T\,E\;\;N\;\;S\;\;I\;\;N\,D\;\;N\;\;I\,C\;\;H\;\;T\;\;G\;\;U\;\;T} \end{array}$$

4. Lösung:

m	n	Division mit Rest	$a = b'$	$b = a' - qb'$
2431	2601	$2431 = 0 \cdot 2601 + 2431$	-46	43
2601	2431	$2601 = 1 \cdot 2431 + 170$	43	-46
2431	170	$2431 = 14 \cdot 170 + 51$	-3	43
170	51	$170 = 3 \cdot 51 + 17$	1	-3
51	17	$51 = 3 \cdot 17 + 0$	0	1
17	0	$\mathrm{ggT}(2431, 2601) = 17$	1	0

Damit wurde berechnet:

$$17 \;=\; \mathrm{ggT}(2431, 2601) \;=\; -46 \cdot 2431 \,+\, 43 \cdot 2601$$

m	n	Division mit Rest	$a = b'$	$b = a' - qb'$
27047	3363	$27047 = 8 \cdot 3363 + 143$	-682	5485
3363	143	$3363 = 23 \cdot 143 + 74$	29	-682
143	74	$143 = 1 \cdot 74 + 69$	-15	29
74	69	$74 = 1 \cdot 69 + 5$	14	-15
69	5	$69 = 13 \cdot 5 + 4$	-1	14
5	4	$5 = 1 \cdot 4 + 1$	1	-1
4	1	$4 = 4 \cdot 1 + 0$	0	1
1	0	$\mathrm{ggT}(27047, 3363) = 1$	1	0

Damit wurde berechnet:

$$1 \;=\; \mathrm{ggT}(27047, 3363) \;=\; -682 \cdot 27047 \,+\, 5485 \cdot 3363$$

5. Lösung: Da zwei gerade Zahlen zumindest den gemeinsamen Teiler 2 besitzen, können sie nicht teilerfremd sein.

6. Lösung: Es gibt mehrere Lösungsmöglichkeiten; zwei sollen hier erläutert werden:

   (a) Multipliziert man die Potenz $(u+1)^k$ aus[1], so erhält man eine Summe mit zahlreichen Summanden von denen genau einer den Wert 1 hat und alle übrigen durch u teilbar sind. Faßt man die durch u teilbaren zusammen und klammert u aus, so erhält man mit einem $a \in \mathbb{Z}$ für die Potenz $(u+1)^k$ die Darstellung

   $$(u+1)^k \;=\; a \cdot u \,+\, 1 \tag{1}$$

   Das liefert wiederum

   $$(u+1)^k \,-\, a \cdot u \;=\; (a \cdot u \,+\, 1) \,-\, a \cdot u \;=\; 1$$

[1] Man könnte den Binomischen Lehrsatz verwenden.

Also:

$$(u+1)^k \; - \; a \cdot u \; = \; 1$$

Gäbe es nun einen gemeinsamen Teiler $d > 1$ von u und $(u+1)^k$, so wäre das auch ein Teiler von 1; und das kann nicht sein. Folglich müssen u und $(u+1)^k$ teilerfremd sein.

(b) Man führt eine vollständige Induktion über den Exponenten k durch.
Für $k = 1$ sind u und $(u+1)^1$ wegen

$$(u+1) \; - \; u \; = \; 1$$

teilerfremd: Ein gemeinsamer Teiler $d > 1$ müßt auch 1 teilen, was nicht möglich ist.
Für $k > 0$ werde angenommen, daß u und $(u+1)^{k-1}$ teilerfremd ist. Da im Induktionsanfang bereits gezeigt wurde, daß u und $u+1$ teilerfremd sind, folgt mit Hilfe eines Hilfssatzes der Vorlesung, daß auch

$$u \qquad \text{und} \qquad (u+1)^k \; = \; (u+1)^{k-1} \cdot (u+1)$$

teilerfremd sind.

7. Lösung:

$$\begin{aligned} 157 &= 31 \cdot 5 + 2 \\ 31 &= 6 \cdot 5 + 1 \\ 6 &= 1 \cdot 5 + 1 \\ 1 &= 0 \cdot 5 + 1 \\ \Rightarrow\; 157 &= (1112)_5 \end{aligned} \qquad \begin{aligned} 785 &= 157 \cdot 5 + 0 \\ 157 &= 31 \cdot 5 + 2 \\ 31 &= 6 \cdot 5 + 1 \\ 6 &= 1 \cdot 5 + 1 \\ 1 &= 0 \cdot 5 + 1 \\ \Rightarrow\; 785 &= (11120)_5 \end{aligned}$$