- **Der Lösungsweg muss ersichtlich sein. Alle Ausrechungen gehören auf das Lösungsblatt. Jede Aufgabe ist auf einer neuen Seite zu beginnen.**
- **Zugelassene Hilfsmittel sind das ausgehändigte Formelbuch *Formeln, Tabellen und Begriffe* sowie ein Taschenrechner (TI 82/83).**
- **Für die Note 6 werden 69 Punkte verlangt.**

Aufgabe 1 *((Bienen und Mandelbäume, 16 Punkte: a)9, b)7))*

Betrachte ein Differentialgleichungssystem einer Symbiose (z.B. Bienen und Mandelbäume), bei dem die Funktionen für die jeweiligen Populationsgrössen x und y zu einem beliebigen Zeitpunkt $t \geq 0$ folgende Differentialgleichungen erfüllen:

$$x'(t) = 0.6x(t) + 0.4y(t)$$
$$y'(t) = 0.2y(t) + 0.8x(t)$$

(a) Bestimme die allgemeine Lösung dieses Differentialgleichungssystems.

(b) Wie lauten die Lösungsfunktionen, wenn zu Beginn ein Bienenvolk mit 40 000 Individuen zu einem Mandelhain mit 10 000 Bumen gebracht wird? Kommentiere das Langzeitverhalten des Systems.

Aufgabe 2 *((Epidemie, 14 Punkte: a)5, b)9))*

Eine einfache Modellierung einer Epidemie führe auf die Differentialgleichung

$$\frac{dK}{dG} = -1 + \frac{p}{rG}$$

wobei K für die Anzahl „Erkrankte" und G für die Anzahl „Gesunde" steht.

(a) Leite obige Differentialgleichung aus folgenden Annahmen her:

- Die Zahl derer, die infiziert werden, ist proportional (Proportionalitätskonstante r) zum Produkt der Gesunden G und Kranken K.
- Aus der Klasse der Kranken gehen mit einem konstanten Faktor — nennen wir ihn p — Individuen in die Klasse der Immunen I über.
- Die Population ist konstant.

Hinweis: Notiere zuerst Gleichungen für $\frac{dK}{dt}$ und $\frac{dG}{dt}$.

(b) Löse obige Differentialgleichung mit den Startwerten G_0 und K_0 nach K. Diskutiere anschliessend das Langzeitverhalten für K. Gibt es einen kritischen Wert, bei dem die Epidemie „stagniert"? In andern Worten: Gibt es einen Wert, ab dem die Zahl der Kranken stetig abnimmt?

Aufgabe 3 *((RSA, 15 Punkte: a)1, b)8, c)6))*

In dieser Aufgabe soll das Verschlsselungsverfahren RSA behandelt werden.

(a) Für was stehen die Buchstaben RSA?

(b) Erkläre die Funktionsweise von RSA mit public key (n, e) und private key d. Kommentiere insbesondere die Wahl bzw. Berechnung von n, e und d. Wieso gilt RSA als sicher? Zeige schliesslich allgemein, dass RSA korrekt arbeitet. Dabei darfst du den kleinen Satz von Fermat als bekannt voraussetzen.

(c) Bestimme mit den Primzahlen 13 und 19 den public key und den private key und verschlüssle anschliessend $\mathtt{C} = 3$. Wähle dazu $e = 17$.

Aufgabe 4 *((Ursprungsaffinitäten, 19 Punkte: a)4, b)3, c)3, d)2, e)7))*

Betrachte im $\mathbb{R}^2$ die Matrizen der affinen Ursprungsabbildungen

$$\sigma : \begin{pmatrix} 1 & \frac{\sqrt{3}}{3} \\ 0 & 1 \end{pmatrix} \quad \text{und} \quad \delta : \begin{pmatrix} \frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & \frac{1}{2} \end{pmatrix}.$$

(a) Beschreibe die Abbildungen σ und δ geometrisch.

(b) Bestimme die Abbildungsmatrix der Verkettung $\sigma \circ \delta$.

(c) Bestimme die Umkehrabbildung von δ und damit das Urbild von $P'\,(1\,|\,1)$.

(d) In welchen Verhältnissen stehen jeweils Flächeninhalte zu ihren Bildflächeninhalten unter der Abbildung σ?

(e) Bestimme alle Fixpunkte und Fixgeraden von σ.

Lsungen

Aufgabe 1 *((Bienen und Mandelbäume, 16 Punkte: a)9, b)7))*

(a) Das Differentialgleichungssystem mit Gleichungen erster Ordnung kann mit der Eigenwert / Eigenvektor-Methode gelöst werden. Setze

$$A = \begin{pmatrix} 0.6 & 0.4 \\ 0.8 & 0.2 \end{pmatrix}.$$

Das charakteristische Polynom ist

$$\chi_A = \lambda^2 - 0.8\lambda - 0.2$$

und liefert die Eigenwerte

$$\lambda_1 = 1 \quad \text{und} \quad \lambda_2 = -0.2$$

mit Eigenvektoren

$$v_1 = (1 \,|\, 1) \quad \text{bzw.} \quad v_2 = (-0.5 \,|\, 1)\,.$$

Daraus erhält man die allgemeine Lösung

$$\begin{aligned} x(t) &= C_1 e^t - 0.5 C_2 e^{-0.2t} \\ y(t) &= C_1 e^t + C_2 e^{-0.2t} \end{aligned}$$

(1Pkt Matrix, 1Pkt CharPoly, 1Pkt Eigenwerte, 2Pkt Eigenvektoren, 4Pkt für die Lösung)

(b) Zu den Anfangswerten $x(0) = 40\,000$ und $y(0) = 10\,000$ gehört das Gleichungssystem

$$\begin{aligned} 40\,000 &= C_1 - 0.5 C_2 \\ 10\,000 &= C_1 + C_2 \end{aligned}$$

woraus $C_1 = 30\,000$ und $C_2 = -20\,000$ folgt. Somit ist

$$\begin{aligned} x(t) &= 30\,000 e^t + 10\,000 e^{-0.2t} \\ y(t) &= 30\,000 e^t - 20\,000 e^{-0.2t} \end{aligned}$$

Für $t \to \infty$ wachsen x und y und streben $x \div y = 1 \div 1$ an.

(1Pkt fär das GlSys, 2Pkt für C_1, C_2, 2Pkt für die Lösung, 2Pkt für $1 \div 1$)

Aufgabe 2 *((Epidemie, 14 Punkte: a)5, b)9))*

(a) Die Bedingungen führen zu

$$\frac{dK}{dt} = rGK - pK \quad \text{und} \quad \frac{dG}{dt} = -rGK.$$

Daraus folgt

$$\frac{\frac{dK}{dt}}{\frac{dG}{dt}} = \frac{dK}{dG} = -1 + \frac{p}{rG}.$$

(2Pkt fr $\frac{dK}{dt}$, 2Pkt für $\frac{dG}{dt}$, 1Pkt für die Lösung)

(b) Separation der Variablen liefert

$$dK = (-1 + \frac{p}{rG})dG.$$

Integration von K_0 bis K bzw. G_0 bis G:

$$\begin{aligned}
\int_{K_0}^{K} dK &= \int_{G_0}^{G} (-1 + \frac{p}{rG})dG \\
K - K_0 &= -G + \frac{p}{r}\ln(G) - (-G_0 + \frac{p}{r}\ln(G_0)) \\
K - K_0 &= G_0 - G + \frac{p}{r}\ln\left(\frac{G}{G_0}\right) \\
K(G) &= K_0 + G_0 - G + \frac{p}{r}\ln\left(\frac{G}{G_0}\right)
\end{aligned}$$

Man stellt fest, dass die Anzahl der Erkrankten ab $\frac{p}{r}$ abnimmt und schliesslich nur Gesunde liefert. Denn es ist

$$\frac{dK}{dG} = 0 = -1 + \frac{p}{rG},$$

also

$$G_{max} = \frac{p}{r},$$

und

$$\frac{dK^2}{d^2G} = -\frac{p}{rG^2}$$

wobei $r > p > 0$

(1Pkt für Separation, 1Pkt für Integralgrenzen, 2Pkt für Grenzen korrekt eingesetzt, 1Pkt für die Lösung $K(G)$, 1Pkt für MaxBedingung, 1Pkt für Max $\frac{p}{r}$, 1Pkt für 2. Ableitung, 1Pkt für Argumentation 2. Ableitung stets negativ)

Aufgabe 3 *((RSA, 15 Punkte: a)1, b)8, c)6))*

(a) RSA steht für die Initialen der Nachnamen der Erfinder: Rivest, Shamir, Adleman

(1Pkt für die Namen)

(b) RSA ist ein asymmetrisches Verschlüsselungsverfahren. D.h. es gibt einen öffentlichen und einen privaten Schlüssel. Der öffentliche Schlüssel (n, e) besteht aus einem Produkt zweier Primzahlen, $n = p \cdot q$ — p, q „genügend" gross, und einer Zahl e — $e = 2^k + 1$, da „einfache" Binärdarstellung die Berechnungen effizient macht —, die teilerfremd zu $(p-1)\cdot(q-1)$ ist. Denn nur falls letzteres gegeben ist, kann ein eindeutiger privater Schlüssel d berechnet werden, der entschlüsselt. d kann mit dem erweiterten Euklid'schen Algorithmus berechnet werden, wenn man p und q kennt. Ist d berechnet, werden p und q vernichtet. Das Verfahren ist nach heutigen Stand der Kenntnisse sicher, da kein Algorithmus bekannt ist, der in „nützlicher" Zeit n faktorisieren kann. Kurz:

- RSA ist asymmetrisch
- $n = pq$ mit p, q prim
- e teilerfremd zu $(p-1)(q-1)$
- d kann mit dem erweiterten Euklidischen Algorithmus berechnet werden, wenn man p und q kennt.

RSA arbeitet korrekt:

Eine message m wird mit e via $c = m^e \mod pq$ verschlüsselt und danach mit $\tilde{m} = c^d \mod pq = (m^e)^d \mod pq$ entschlüsselt. d wurde so gewählt, dass

$$e \cdot d = k \cdot (p-1)(q-1) + 1$$

erfüllt ist. Damit gilt nun für m Modulo p

$$m^{ed} - m = m^{k(p-1)(q-1)+1} - m = (m^{(p-1)})^{k(q-1)}m - m = 1^{k(q-1)}m - m = 0$$

wobei der kleine Satz von Fermat, $a^{p-1} \mod p = 1$, verwendet wurde. Für q gilt dies analog. Da also p und q $m^{ed} - m$ teilen, ist auch ihr Produkt ein Teiler. Somit ist

$$m^{ed} \mod pq \equiv m$$

(1Pkt für $n = pq$ mit p, q prim, 1Pkt für e teilerfremd zu $(p-1)(q-1)$, 1Pkt für d mit erweitertem Euklidischen Algorithmus, 1Pkt Argument für die Sicherheit von RSA, 1Pkt m^{ed}, 1Pkt $ed = k(p-1)(q-1) + 1$, 1Pkt Anwendung Fermat, 1Pkt Resultat m bzw. 0.)

(c) $n = pq = 247$, public key $(247, 17)$. $(p-1)(q-1) = 216$, was teilerfremd zu 17 ist, womit sich der Entschlüsselungsexponent d bestimmen lässt:

$$\begin{aligned} 216 &= 12 \cdot 17 + 12 \\ 17 &= 1 \cdot 12 + 5 \\ 12 &= 2 \cdot 5 + 2 \\ 5 &= 2 \cdot 2 + 1 \end{aligned}$$

Erweiterung:

$$\begin{aligned}
1 &= 5 - 2 \cdot 2 = 5 - 2(12 - 2 \cdot 5) = -2 \cdot 12 + 5 \cdot 5 \\
&= -2 \cdot 12 + 5(17 - 1 \cdot 12) = 5 \cdot 17 - 7 \cdot 12 \\
&= 5 \cdot 17 - 7 \cdot (216 - 12 \cdot 17) \\
&= -7 \cdot 216 + 89 \cdot 17
\end{aligned}$$

liefert $d = 89$.

Cipher $c = 3^{13} \mod 323 = 318$

(1Pkt $n = 247$, 1Pkt $(p-1)(q-1) = 216$, 1Pkt Euclid, 1Pkt Erweiterung Euklid, 1Pkt $d = 89$, 1Pkt $c = 165$)

Aufgabe 4 *((Ursprungsaffinitäten, 19 Punkte: a)4, b)3, c)3, d)2, e)7))*

(a) σ ist eine Scherung an der x-Achse; der Scherungswinkel bezüglich der Vertikalen ist $-\arctan(\frac{\sqrt{3}}{3}) = -30!`$.

Wegen $\det \delta = 1$ und den Zeilenquadratsummen mit Wert 1 ist δ eine Drehung; der Drehwinkel ist $\arccos(\frac{1}{2}) = 60!`$.

(1Pkt für Scherung an x-Achse, 1Pkt für Scherungswinkel, 1Pkt für Drehung, 1Pkt für Drehwinkel)

(b) Die Verkettung $\sigma \circ \delta$ entspricht der Multiplikation $\sigma \cdot \delta$:

$$\begin{pmatrix} 1 & \frac{\sqrt{3}}{3} \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & \frac{1}{2} \end{pmatrix} = \begin{pmatrix} 1 & -\frac{\sqrt{3}}{3} \\ \frac{\sqrt{3}}{2} & \frac{1}{2} \end{pmatrix}$$

(1Pkt für Multiplikation, 2Pkt für das Resultat)

(c) Die Inverse von δ ist

$$\begin{pmatrix} \frac{1}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & \frac{1}{2} \end{pmatrix}$$

Das Urbild ist $\left(\frac{1+\sqrt{3}}{2} \mid \frac{1-\sqrt{3}}{2}\right)$.

(1Pkt für die Inverse, 2Pkt für das Urbild)

(d) Es gilt $F' = \det(\sigma) \cdot F$ wobei $\det(\sigma) = 1$.

(1Pkt für die det, 1Pkt für die Beziehung)

(e) Zur Beantwortung dieser Frage untersucht man die Eigenwerte und Eigenvektoren von σ. Das charakteristische Polynom ist

$$\chi_\sigma = \lambda^2 - 2\lambda + 1$$

und damit $\lambda_{1,2} = 1$ doppelter Eigenwert. Somit gibt es eine Fixpunktgerade und weitere Fixgeraden, die parallel zur Fixpunktgeraden verlaufen. Die Richtung gibt der Eigenvektor vor. Die erste Zeile liefert

$$0 \cdot x + \frac{\sqrt{3}}{3} y = 0$$

also x beliebig und $y = 0$, was der x-Achse als Fixpunktgeraden entspricht. Die weiteren Fixgeraden sind dann $y = b$ mit $b \in \mathbb{R}$, also alle Parallelen zur x-Achse.

(1Pkt für das CharPoly, 1Pkt für den Eigenwert, 1Pkt für die Eigenvektorgleichung, 1Pkt für einen Eigenvektor, 1Pkt für die Fixpunktgerade, 1Pkt für weitere Fixgeraden, 1Pkt für die Fixgeradengleichungen)