Merkzettel für Mathe I

erstellt aus Vorlesungsskripten,
Büchern und Übungsblättern

Die Repertoire – Methode:
(vorgehensweise anhand eines Beispiels)

Gegeben seien die Rekursionsformeln
a.) $g(1) = \alpha$
b.) $g(n+1) = (n+1) \cdot g(n) + \beta \cdot n$

Ziel ist folgende Darstellung zu finden :
$g(n) = A(n) \cdot \alpha + B(n) \cdot \beta + ...$

Gegeben sind folgende Ansätze :
1.) $g(n) = n!$
2.) $g(n) = 1$

Diese Ansätze werden nun in die Rekursionsformeln eingesetzt :
1.) Ansatz $g(n) = n!$
a.) $g(1) = \alpha \Rightarrow \alpha = 1! \Rightarrow \alpha = 1$
b.) $(n+1)! = (n+1) \cdot n! + \beta \cdot n$
(nach β aufgelöst)
$\beta = 0$
Nun wird in die Darstellung eingesetzt, unter Beachtung des 1.) Ansatzes $g(n) = n!$:
$g(n) = A(n) \cdot \alpha + B(n) \cdot \beta \Rightarrow$
$n! = A(n) \cdot 1 + B(n) \cdot 0 \Rightarrow$
$A(n) = n!$

2.) Ansatz $g(n) = 1$
a.) $g(1) = \alpha \Rightarrow \alpha = 1$
b.) $1 = (n+1) \cdot 1 + \beta \cdot n$
(nach β aufgelöst)
$\beta = -1$
Nun wird in die Darstellung eingesetzt, unter Beachtung des 2.) Ansatzes $g(n) = 1$:
$g(n) = A(n) \cdot \alpha + B(n) \cdot \beta \Rightarrow$
$1 = A(n) \cdot 1 + B(n) \cdot (-1) \Rightarrow$
$B(n) = A(n) - 1$
Unter Verwendung des Ansatzes 1.) wird $A(n)$ eingesetzt :
$B(n) = n! - 1$

Eingesetzt in die geforderte Darstellung ergibt sich folgende Lösung :
$g(n) = A(n) \cdot \alpha + B(n) \cdot \beta \Rightarrow g(n) = n! \cdot \alpha + (n! - 1) \cdot \beta$

Komplexe quadratische Gleichungen:

$$x_{1/2} = \frac{-b \pm \sqrt{b^2 - 4 \cdot a \cdot c}}{2 \cdot a}; \qquad x_{1/2} = -\frac{p}{2} \pm \sqrt{\left(\frac{p}{2}\right)^2 - q}$$

$$\tan^{-1}\alpha = \frac{Gegenkathete}{Ankathete}; \qquad e^{i\varphi} = \cos\varphi + i\sin\varphi$$

Potenzen:

$$a^m \cdot a^n = a^{m+n}$$

$$a^n \cdot b^n = (a \cdot b)^n$$

$$\frac{a^m}{a^n} = a^{m-n}$$

$$(a^m)^n = a^{m \cdot n}$$

Größter gemeinsamer Teiler d:
(vorgehensweise anhand eines Beispiels)

Gesucht wird die Darstellung $d = a \cdot 405 + b \cdot 435$
(erweiterter euklidischer Algorithmus)

a.) $435 = 1 \cdot 405 + 30$
b.) $405 = 13 \cdot 30 + 15$
c.) $30 = 2 \cdot 15 + 0$

Aus den Ergebnisse werden nun die Matrizen der Form $\begin{pmatrix} 0 & 1 \\ 1 & -q \end{pmatrix}$ gebildet

a.) $Q_1 = \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}$

b.) $Q_2 = \begin{pmatrix} 0 & 1 \\ 1 & -13 \end{pmatrix}$

c.) $Q_3 = \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix}$

Nun werden die Matrizen in der Reihenfolge Q_3, Q_2, Q_1 multipliziert

$$Q_3 \cdot Q_2 \cdot Q_1 = \begin{pmatrix} -13 & 14 \\ 27 & -29 \end{pmatrix}$$

Es kann nun folgende Gleichung aufgestellt werden

$$\begin{pmatrix} 15 \\ 0 \end{pmatrix} = \begin{pmatrix} -13 & 14 \\ 27 & -29 \end{pmatrix} \cdot \begin{pmatrix} 435 \\ 405 \end{pmatrix}$$

Hieraus kann die Gleichung abgelesen werden :

$15 = -13 \cdot 435 + 14 \cdot 405$

$(0 = 27 \cdot 435 - 29 \cdot 405)$

Lineare Algebra:

dim Zeilenraum A = Zeilenrang A = Spaltenrang A = dim Spaltenraum A = rg$A$ (= Anzahl der Zeilen, die nicht 0 werden)
dim Nullraum A = dim Ker A = n - rg A (= Anzahl der freiwählbaren Elemente)

Basis des Zeilenraums, Spaltenraums von A
→ Umformen in die reduzierte Zeilenstufenform
⇒ Zeilenraumbasis sind die Zeilen der reduzierten Zeilenstufenform, die nicht 0 sind
⇒ Spaltenraumbasis sind die Spalten von A, die in der reduzierten Zeilenstufenform eine führende 1 haben.
Basis des Nullraums (= Kern$A$) von A
→ A in reduzierte Zeilenstufenform bringen
→ entstehende Gleichungen hinschreiben
→ Umformen, so daß sich die festen Elemente aus freiwählbaren Elementen kombinieren
→ Lösung hinschreiben

$$N(A)=\left\{\left.\begin{pmatrix} -x_2-\frac{2}{3}x_5 \\ x_2 \\ -x_5-3x_6 \\ \frac{1}{3}x_5 \\ x_5 \\ x_6 \end{pmatrix}\right| x_2,x_5,x_6\in R\right\}=\left\{x_2\begin{pmatrix}-1\\1\\0\\0\\0\\0\end{pmatrix}+x_5\begin{pmatrix}-\frac{2}{3}\\0\\-1\\\frac{1}{3}\\1\\0\end{pmatrix}+x_6\begin{pmatrix}0\\0\\-3\\0\\0\\1\end{pmatrix}\ x_2,x_5,x_6\in R\right\}$$

Eigenwerte Diagonalisierung:
(vorgehensweise anhand eines Beispiels)

$$A=\begin{pmatrix}12 & -6\\ -6 & 7\end{pmatrix}$$

→ $\det(A-\lambda\cdot I)=0$ berechnen
→ Eigenwerte:
$\lambda_1=16,\ \lambda_2=3$
→ Eigenvektoren:

$$\vec{x}_1=\begin{pmatrix}-3\\2\end{pmatrix}$$

$$\vec{x}_2=\begin{pmatrix}2\\3\end{pmatrix}$$

→ Orthonormierung:

$$\vec{x}_1=\sqrt{(-3)^2+(2)^2}=\sqrt{13}=\sqrt{(2)^2+(3)^2}=\vec{x}_2$$

$$\rightarrow \vec{x}_1=\frac{1}{\sqrt{13}}\cdot\begin{pmatrix}-3\\2\end{pmatrix}$$

$$\rightarrow \vec{x}_2=\frac{1}{\sqrt{13}}\cdot\begin{pmatrix}2\\3\end{pmatrix}$$

Matrix aus beiden Vektoren bilden, so daß die Determinante 1 ist
(wenn Determinante -1, $\vec{x}_1$ durch $-\vec{x}_1$ ersetzen)

$\Rightarrow P^t\cdot P=E$ und $P^tAP=\begin{pmatrix}\lambda_1 & 0\\ 0 & \lambda_2\end{pmatrix}$ die gewünschte Eigenschaft

$$\Rightarrow P=\begin{pmatrix}16 & 0\\ 0 & 3\end{pmatrix}$$

Methode der kleinsten Quadrate:

$(A^T \cdot A) \cdot \vec{x} = A^T \cdot \vec{b}$
$\rightarrow$ Gleichungssystem lösen

RSA Verschlüsselung:

Gegeben :
$N = 407$ (Teil des öffentlichen Schlüssels)
$e = 103$ (Teil des öffentlichen Schlüssels)
$p = 11$
$q = 37$
verschlüsselte Botschaft : 148

da $\varphi(N) = (p-1)(q-1)$
$\Rightarrow \varphi(407) = 10 \cdot 36 = 360$

Ziel ist, den privaten Schlüssel des Empfängers zu finden, um die verschlüsselte Botschaft zu entschlüsseln

$ggT(360;103) = 1$ (ist immer so)
finde nun die Darstellung $1 = a \cdot 360 + b \cdot 103$ mittels erweiterten euklidischen Algorithmus

$$\Rightarrow \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} -2 & 7 \\ 103 & -360 \end{pmatrix} \cdot \begin{pmatrix} 360 \\ 103 \end{pmatrix}$$

$\Rightarrow 1 = -2 \cdot (360) + 7 \cdot (103)$
$\Rightarrow 7$ ist das 360 - modular Inverse zu 103
$\Rightarrow 7$ ist der gesuchte private Schlüssel

x = Klartext
y = verschlüsselte Botschaft (hier 148)
$priv$ = privater Schlüssel (hier 7)
N = Teil des öffentlichen Schlüssels (hier 407)
e = Teil des öffentlichen Schlüssels (hier 103)

Entschlüsseln :
$x = y^{priv} \bmod N \Rightarrow x = 148^7 \bmod 407 \Rightarrow x = 333$

Verschlüsseln :
$y = x^e \bmod N \Rightarrow y = 333^{103} \bmod 407$