

Computergestützte Mathematik zur linearen Algebra – 1. Übungsblatt

Aufgabe 0: (JUPYTER und SPYDER starten) Diese Aufgabe gibt KEINEN Punkt!

- (a) (1) Starten Sie die JUPYTER-Oberfläche.
- (2) Erstellen Sie ein neues Notebook und nennen Sie es `Uebung01`.
- (3) Schreiben Sie „*Dies ist das erste Übungsblatt*“ in die erste Zeile.
- (b) (1) Erstellen Sie in Ihrem Homeverzeichnis einen Ordner `CompLA` und darin einen Ordner `Blatt01`.
- (2) Starten Sie SPYDER.

Aufgabe 1: (Erste Schritte)

Lösen Sie diese Aufgabe im JUPYTER Notebook aus Aufgabe 0 (a). Bestimmen Sie mit dem Befehl `type()` den Typ der folgenden Ausdrücke:

- (a) `3`
- (b) `3.`
- (c) `3 + 0j`
- (d) `'Dagobert'`
- (e) `(1, 2, 3)`
- (f) `range(11)`
- (g) `[1, 2, "Daisy"]`
- (h) `set([3, 1, 4, 1, 5])`
- (i) `print('Donald')`
- (j) `{0 : 1, 4 : 'D', -3 : [1, 2, 3]}`

Aufgabe 2: (Ausdrücke verstehen)

Überlegen Sie sich die Ergebnisse der folgenden mathematischen Ausdrücke und überprüfen Sie diese im JUPYTER Notebook aus Aufgabe 0 (a).

Hinweis: Sie können die Ausdrücke nicht direkt in die Eingabezeile tippen, sondern müssen sie zuerst in PYTHON Syntax umschreiben.

- (a) $(12.9 + 7.1) \cdot 5$
- (b) $\frac{2}{3} + \frac{2}{0.1}$
- (c) $(5 + 7i) \cdot (2 - i)$
- (d) 2^4
- (e) $5 + 11 \bmod 12$
- (f) $\frac{5(3-9)}{7 + \frac{-15}{3}}$

Informieren Sie sich mit Hilfe von `?range` oder `help(range)` über den Befehl `range`. Überlegen Sie sich damit die Ergebnisse der folgenden Ausdrücke und überprüfen Sie diese wieder im JUPYTER Notebook.

- (g) `list(range(5))`
- (h) `set(range(5))`
- (i) `list(range(1, 5, 1))`
- (j) `set(range(1, 5, 1))`
- (k) `list(range(5, 1, -1))`
- (l) `set(range(5, 1, -1))`

Aufgabe 3: (*Slicing*)

Erstellen Sie im JUPYTER Notebook aus Aufgabe 0 (a) folgendes Objekt des Typs `list`:

`a = [3, 1, 4, 1, 5, 9, 2, 6, 5, 3, 5]`

Greifen Sie nun mit Hilfe von *Slices* auf folgende Elemente zu:

- (a) Das dritte bis achte Element.
- (b) Die Elemente mit ungerader Nummer.
- (c) Das erste, vierte, siebte und zehnte Element.
- (d) Alle Elemente ab dem zweiten.
- (e) Das elfte bis fünfte Element (also rückwärts).
- (f) Das vor-, viert-, sechst- und achtletzte Element.

Aufgabe 4: (Variablen)

Wird jedem Buchstaben eine Zahl M zugeordnet, etwa a der Zahl 10, b der Zahl 11 und c der Zahl 12, usw., so kann Alice an Bob eine mit Hilfe der geteilten geheimen Schlüssel $s = 17$ und $p = 97$ eine verschlüsselte Nachricht senden, die Bob entschlüsselt.

Sie gehen dabei wie folgt vor:

- (a) Alice ordnet einem Buchstaben eine Zahl M zu.
- (b) Nun verschlüsselt sie diese Zahl, indem sie $E = (M \cdot s) \bmod p$ berechnet.
- (c) Alice sendet E an Bob.
- (d) Bob hat inzwischen $s^{-1} \bmod p$ berechnet, die modulare multiplikative Inverse von s , das ist die Inverse von s im Ring $\mathbb{Z}/p\mathbb{Z}$,
- (e) und berechnet $M = (E \cdot s^{-1}) \bmod p$.

Korrigieren Sie den angegebenen Pythonalgorithmus, der dieses Vorgehen umsetzt.

```
# dictionary mit der Zuordnung Buchstabe Zahl
code = {'a': 10, 'b': 11, 'c': 12}
# Schlüssel
p = 97
s = 17

M = code['b'] # codierte Nachricht
print(M)
E = (M * s) % p # verschlüsselte Nachricht
print('chiffrierte Nachricht', E)
sinv = pow(s, -1, p) # modulare Inverse von s / Inverse von s in F_p
M = (E * sinv) % p
print M
```

Obige Pythondatei finden Sie bei den Übungsblättern auf der Homepage.
<http://www.am.uni-duesseldorf.de/~schaedle/lehre/ws2024/CompLA>

Besprechung in den Übungen vom 14.10.2022 bis 18.10.2022.