

<p>4. Übungsblatt Diskrete Strukturen (Winter 2019/20)</p>
--

Bauhaus-Universität Weimar, Professur für Mediensicherheit

Dr. Stefan Lucks, Jannis Bossert

URL: <http://www.uni-weimar.de/de/medien/professuren/mediensicherheit/teaching>

Abgabe: Bis zum 10. Dezember 2019 vor Beginn der Übung oder per E-Mail an jannis.bossert@uni-weimar.de. Lösungen sind bevorzugt in LaTeX zu verfassen. Ein Template finden Sie auf der Übungsseite der Veranstaltung.

Aufgabe 1 – Generatoren (4 Punkte)

Geben Sie alle Generatoren (erzeugende Elemente) an von:

a) $(\mathbb{Z}_{11}^*, \cdot)$

b) $(\mathbb{Z}_{14}^*, \cdot)$

Bedenken Sie, dass die Multiplikation in \mathbb{Z}_n^* modulo n passiert.

Aufgabe 2 – Ordnung (4 Punkte)

Erklären Sie zunächst in eigenen Worten, was die Ordnung einer Gruppe und was die Ordnung eines Elementes einer Gruppe ist. Erläutern Sie außerdem, was die eulersche φ -Funktion $\varphi(n)$ berechnet.

Bestimmen Sie anschließend, die Ordnung von

a) $(\mathbb{Z}_{12}^*, \cdot)$

b) 5 in $(\mathbb{Z}_{14}^*, \cdot)$

c) $\varphi(1999)$

Aufgabe 3 – Gruppeneigenschaften (6 Punkte)

Lösen Sie die folgenden Aufgaben zum Thema Gruppeneigenschaften.

a) Untersuchen Sie die folgende potentielle Gruppe $(\{0, 1\}^n, \oplus)$ auf Ihre Gruppeneigenschaften. $\{0, 1\}^n$ meint dabei n -bit Werte und \oplus XOR.

b) Untersuchen Sie die folgende potentielle Gruppe auf ihre Gruppeneigenschaften:
 (\mathbb{Z}_{13}, \circ) mit $a, b \in \mathbb{Z}_{13}$ und $a \circ b := (2 \cdot a + 2 \cdot b) \bmod 13$.

c) Sei $\text{Dlog}_{2,11}(a)$ der diskrete Logarithmus zur Basis 2 in \mathbb{Z}_{11} . Es gilt für alle $a \in \mathbb{Z}_{10}$:
 $\text{Dlog}_{2,11}(2^{a \bmod 10} \bmod 11) = a$. Zum Beispiel ist $\text{Dlog}_{2,11}(5) = 4$, denn $2^4 \bmod 11 \equiv 5$.
Untersuchen Sie die folgende potentielle Gruppe auf ihre Gruppeneigenschaften:
 (\mathbb{Z}_{10}, \circ) mit $a, b \in \mathbb{Z}_{10}$ und $a \circ b := \text{Dlog}_{2,11}(2^a \cdot 2^b \bmod 11)$.

Aufgabe 4 – Eindeutigkeit (4 Punkte)

Beweisen Sie Satz 52 und Satz 53 aus der Vorlesung.

Satz 52 (Eindeutigkeit des neutralen Elements)

In einer Halbgruppe gibt es höchstens ein neutrales Element.

Satz 53 (Eindeutigkeit des Inversen)

In einem Monoid gibt es zu jedem Element höchstens ein Inverses. Hat x ein Inverses x^{-1} , dann ist x selbst das Inverse von x^{-1} .

Aufgabe 5 – Fermat-Test + RSA (Programmieraufgabe) (5 Punkte)

Implementieren Sie den Fermat-Test und den RSA-Algorithmus aus der Vorlesung (Folien 134 und 123) in Python. Das Programm soll dabei vier Werte p , q , x und k als Kommandozeilenparameter entgegennehmen und folgende Funktionalität bieten:

- Behandlung fehlerhafter Eingaben, z. B.: falsche Anzahl oder falscher Typ von Kommandozeilenparametern.
- Testen mittels des Fermat-Tests, ob p und q prim sind. Die Anzahl an verwendeten Zufallszahlen soll dabei k entsprechen. k soll optional sein. Wenn p und/oder q keine Primzahlen sind, soll ihr Programm `p = <xx> is not prime` bzw. `q = <xx> is not prime` ausgeben.
- Berechnen des RSA Modulus $n = p \cdot q$ und der φ -Funktion $\varphi(n) = (p - 1) \cdot (q - 1)$.
- Auswahl des kleinstmöglichen öffentlichen Exponenten $e \in \mathbb{N}_{\varphi(n)}^*$ mit $\text{ggT}(\varphi(n), e) = 1$.
- Berechnen des geheimen Exponenten d mit Hilfe des Erweiterten Euklidischen Algorithmus' (s. Folien 106 ff.).
- Verschlüsseln von Nachrichten M mit (e, n) mit $C = M^e \bmod n$.
- Entschlüsseln von Chiffretexten C mit (d, n) mit $M' = C^d \bmod n$.

Beispielaufruf:

```
python3 rsa_<xxxxxxx>.py --mode=encrypt 73 67 507
3648
python3 rsa_<xxxxxxx>.py --mode=encrypt 73 67 507 -k 15
3648
python3 rsa_<xxxxxxx>.py --mode=decrypt 73 67 3648
507
python3 rsa_<xxxxxxx>.py --mode=encrypt 72 67 3648
p = 72 is not prime
python3 rsa_<xxxxxxx>.py --mode=encrypt 73 66 3648
q = 66 is not prime
```

Schicken Sie Ihre Lösung als Anhang einer E-Mail als Pythondatei

`rsa_<IhreMatrikelnummer>.py`

an `eik.list(at)uni-weimar.de` mit dem Betreff **[DS WS2018/19 Beleg 4]**. Es reicht für **IhreMatrikelnummer** eine Matrikelnummer Ihrer Gruppe. Die vollständigen Namen und Matrikelnummern sollen als Kommentar in der Pythonabgabe stehen.