# 3. Übungsblatt
# Diskrete Strukturen (Winter 2019/20)

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 26. November 2019 vor Beginn der Übung oder per E-Mail an `jannis.bossert(at)uni-weimar.de`. Lösungen sind bevorzugt in LaTeX zu verfassen. Ein Template finden Sie auf der Übungsseite der Veranstaltung.

**Aufgabe 1 – Primzahlen und $k$-glatte Zahlen (6 Punkte)**
Sei $k \in \mathbb{N}$ und $\pi(k)$ die Anzahl der Primzahlen $p_1, \ldots, p_{\pi(k)} \leq k$ bis $k$. Zum Beispiel ist $\pi(5) = 3$. Eine Zahl $m \in \mathbb{N}$ heißt $k$-glatt wenn all ihre Primteiler kleiner gleich $k$ sind:

$$m = p_1^{e_1} \cdot p_2^{e_2} \cdot \cdots \cdot p_{\pi(k)}^{e_{\pi(k)}}.$$

wobei $e_1, \ldots, e_{\pi(k)} \in \mathbb{N}_0$. Wir definieren $P_k \stackrel{\text{def}}{=} p_1 \cdot p_2 \cdot \cdots \cdot p_{\pi(k)}$.
Beweisen oder widerlegen Sie die folgenden Aussagen. Um eine Aussage zu widerlegen, reicht es aus, ein Gegenbeispiel zu nennen.

a) Für jedes $k \geq 3$ gibt es unendlich viele $k$-glatte Zahlen.

b) Für jedes $k \geq 3$ gibt es unendlich viele $k$-glatte Primzahlen.

c) Für jedes $k \geq 3$ gibt es unendlich viele Zahlen $m \in \mathbb{N}$, die nicht $k$-glatt sind.

d) $P_k$ ist die größte $k$-glatte Zahl.

e) Ist $m \in \mathbb{N}$ $k$-glatt, dann ist auch $(m \cdot P_k)$ $k$-glatt.

f) Ist $m \in \mathbb{N}$ $2k$-glatt, dann ist $m$ $k$-glatt.

**Aufgabe 2 – Multiplikatives Inverses (4 Punkte)**
Im Folgenden seien Paare $(a, b)$ mit $a, b \in \mathbb{Z}_n$ gegeben. Ermitteln Sie nachvollziehbar jeweils alle Werte für $n \in \mathbb{N}$ für die gilt: $a^{-1} \equiv b \bmod n$.

a) $(11, 13)$

b) $(7, 42)$

c) $(3, 25)$

d) $(17, 17)$

**Aufgabe 3 – Chinesischer Restsatz (4 Punkte)**
Ermitteln Sie aale Zahlen $n < 500000$ für die gilt:

$$n \bmod 13 = 11$$
$$n \bmod 25 = 17$$
$$n \bmod 7 = 5$$
$$n \bmod 111 = 40.$$

Sollten Sie das multiplikative Inverse einer Zahl benötigen, verwenden Sie den erweiterten euklidischen Algorithmus und geben Sie Ihren Rechenweg an. Sie können Ihr Script aus Aufgabe 5 verwenden, stellen Sie jedoch sicher, dass dieses korrekt ist. Sollte Ihr Script für Aufgabe 5 fehlerhaft sein, werden hier entstehende Fehler nicht als Folgefehler gewertet!

**Aufgabe 4 – Gruppentheorie (4 Punkte)**
Untersuchen Sie die folgenden Paare auf ihre Gruppeneigenschaften:

a) $(\mathbb{N}, *)$

b) $(\mathbb{Z}, *)$

c) $(\mathbb{Q} \setminus \{0\}, *)$

Geben Sie außerdem an, unter welchen Umständen $(\mathbb{Z}_n \setminus \{0\}, *)$ eine Gruppe ist.

**Aufgabe 5 – Erweiterter Euklid (4 Punkte)**
Implementieren Sie den Erweiterten Euklidischen Algorithmus aus der Vorlesung (Kapitel 2.5, Folie 100ff.) in Python. Das Programm soll dabei zwei Zahlen $x$, $y$ als Kommandozeilenparameter entgegennehmen und $(d, a, b)$ zurückgeben mit $d = \mathrm{ggT}(x, y)$ und $ax + by = d$.
**Beispielaufrufe:**

```
# python3 xggt_123456.py 33 27
3,  -4,   5
# python3 xggt_123456.py 3343 77
1, -12, 521
# python3 xggt_123456.py 1234 57
1, -20, 433
# python3 xggt_123456.py 57 57
57,  0,   1
# python3 xggt_123456.py 57 1234
1, 433,  -20
# python3 xggt_123456.py 57 1
1,   0,   1
```

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

**xggt_<IhreMatrikelnummer>.py**

an **jannis.bossert(at)uni-weimar.de** mit dem Betreff **[DS WS2019/20 Beleg 3]**. Es reicht für **IhreMatrikelnummer** eine Matrikelnummer Ihrer Gruppe. Die vollständigen Namen und Matrikelnummern sollen als Kommentar in der Pythonabgabe stehen.