3. Übungsblatt
Diskrete Strukturen (Winter 2018/19)

Bauhaus-Universität Weimar, Professur für Mediensicherheit
Dr. Stefan Lucks, Nathalie Dittrich
URL: `http://www.uni-weimar.de/de/medien/professuren/mediensicherheit/teaching`

Abgabe: Bis zum 27. November 2018 vor Beginn der Übung oder per E-Mail an `eik.list(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) $(5, 13)$

b) $(10, 10)$

c) $(14, 8)$

d) $(17, 10)$

Aufgabe 3 – Multiplikatives Inverses (4 Punkte)
Berechnen Sie für die folgenden Tupel (a, b) jeweils nachvollziehbar den größten gemeinsamen Teiler $\mathrm{ggT}(a, b)$ sowie das multiplikative Inverse $a^{-1} \bmod b$ an *oder* begründen Sie nachvollziehbar warum kein multiplikatives Inverses existiert.

a) $(27, 128)$

b) $(21, 162)$

c) $(123, 1234)$

d) $(511, 5173)$

Aufgabe 4 – Primzahlendichte (2 Punkte)
Im Folgenden ist ein Beispiel einer Liste von aufeinanderfolgenden, zusammengesetzten Zahlen (d.h. keine Primzahlen) angegeben:

$$200, 201, 202, 203, 204, 205, 206, 207, 208, 209, 210$$

Zeigen *oder* widerlegen Sie kurz nachvollziehbar, dass es für alle natürlichen Zahlen $n \in \mathbb{N}$ eine solche Liste der Länge n gibt. *Hinweis: Betrachten Sie große Zahlen* $> n!$.

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, -20, 433
# python3 xggt_123456.py 57 1
1,   0,   1
```

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

`xggt_<IhreMatrikelnummer>.py`

an **`eik.list(at)uni-weimar.de`** mit dem Betreff **`[DS WS2018/19 Beleg 3]`**. Es reicht für **`IhreMatrikelnummer`** eine Matrikelnummer Ihrer Gruppe. Die vollständigen Namen und Matrikelnummern sollen als Kommentar in der Pythonabgabe stehen.