3. Übungsblatt
Diskrete Strukturen (WS 14/15)

Bauhaus-Universität Weimar, Professur für Mediensicherheit
Prof. Dr. Stefan Lucks, Christian Forler, Eik List
URL: `https://www.uni-weimar.de/de/medien/professuren/mediensicherheit/teaching/ws-2014/diskrete-strukturen-vorlesung/`

Abgabe und Besprechung: 18.11.2014 (13:30 Uhr) in der Übung

Hinweise:

- Bei Beweisen ist es wichtig, dass sie nachvollziehbar sind! Liegt also eine Folgerung begründet in einer Definition oder einem Satz, so sollte diese/der mit angegeben werden.
  Beispiel:
  $$a \bmod n = b \bmod n \overset{Def.23}{\Rightarrow} a \equiv b \pmod{n}.$$
- Für Programmieraufgaben: Parameter werden stets als Kommandozeilen-Parameter übergeben.
- Bitte verwenden Sie ausschließlich Büroklammern oder Heftklammern und **keine** Hefter, Folien, Umschläge etc.
- Bitte keine Schmierzettel abgeben und den Namen leserlich schreiben.

Aufgabe 1 (4 Punkte) Multiplikatives Inverse
Berechnen Sie mit Stift und Papier für die folgenden Elemente/Zahlen jeweils das Multiplikative Inverse oder begründen Sie weshalb es nicht existiert.

a) 9 mod 48

b) 16 mod 21

c) 21 mod 113

d) 220 mod 221

Aufgabe 2 (2 Punkte) Das 555-Problem
Berechnen Sie $5^{5^5} \bmod 12$ mit Papier und Stift ohne Computer und Taschenrechner. Geben Sie ihren Rechenweg an.

Aufgabe 3 (2+2+2 Punkte) Beweis von Satz 24 aus der Vorlesung
Zeigen Sie die Gültigkeit der folgenden Aussagen:

a) $(a - b) \bmod n = ((a \bmod n) - (b \bmod n)) \bmod n$

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

c) $a^d \bmod n = (a^{d-x} \cdot a^x) \bmod n = ((a^{d-x} \bmod n) \cdot (a^x \bmod n)) \bmod n$

Aufgabe 4 (2+2 Punkte) Größter gemeinsamer Teiler
Zeigen Sie die beiden folgenden Aussagen:

a) Für alle $a, b, n \in \mathbb{N}$ gilt: Aus $n|ab$ und $\mathrm{ggT}(a, n) = 1$ folgt $n|b$. (Satz 30)

b) Für alle $a, b, k \in \mathbb{N}$ gilt: $\mathrm{ggT}(ka, kb) = k \cdot \mathrm{ggT}(a, b)$.

Aufgabe 5 (4 Punkte) Erweiterter Eukild (Programmieraufgabe)
Implementieren Sie den Erweiterte Euklidische Algorithmus aus der Vorlesung (Kapitel 2.5, Folie 117) in Python. Das Programm soll dabei zwei Zahlen a, b als Kommandozeilenparameter entgegennehmen und (d, x, y) mit $d = \text{ggT}(a, b)$ und $ax + by = d$.

Bevor Sie Ihre Implementation einreichen sollten sie die folgenden Tests korrekt beantworten.

Testfall	**Erwartetes Ergebnis**
xggT(33, 27)	(3, -4, 5)
xggT(3343, 77)	(1, -12, 521)
xggT(1234, 57)	(1, -20, 433)
xggT(57, 57)	(57, 0, 1)
xggT(57, 1234)	(1, 433, -20)
xggT(57, 1)	(1, 0, 1)
xggT(1, 57)	(1, 1, 0)

Beispielaufruf:
```
# python3 xggt_123456.py 33 27
(3,-4,5)
```

(*Abgabe:* Schicken Sie Ihre Lösung als Anhang einer E-Mail `xggt_<MatrNr>.py` an `christian.forler@uni-weimar.de` mit dem Betreff `Erweiterter Euklid`.)