3. Übungsblatt
Diskrete Strukturen (WS 11/12)

Bauhaus-Universität Weimar, Professur für Mediensicherheit
Prof. Dr. Stefan Lucks, Jakob Wenzel
Url: `http://www.uni-weimar.de/cms/medien/mediensicherheit`

Abgabe und Besprechung: 15.11.2011 (15:15 Uhr in der Übung)

Aufgabe 1 (5 Punkte) Zeigen Sie, dass folgende Aussagen gültig sind. Es sei $n \in \mathbb{N}$.

a) **Reflexivität:** $a \equiv a \ (\ mod\ n)$.

b) **Symmetrie:** $a \equiv b \ (\ mod\ n) \Leftrightarrow b \equiv a \ (\ mod\ n)$.

c) **Transitivität:** $a \equiv b \ (\ mod\ n) \wedge b \equiv c \ (\ mod\ n) \Rightarrow a \equiv c \ (\ mod\ n)$.

d) **Regel vom Vielfachen:** Für alle $a, b \in \mathbb{N}$ mit $a > b$ gilt: $(a \equiv b \ (\ mod\ n)) \Leftrightarrow n|(a - b)$.

Aufgabe 2 (6 Punkte) Zeigen Sie, dass folgende Aussagen gültig sind oder bringen Sie ein Gegenbeispiel, falls eine Aussage ungültig ist. Es sei $n \in \mathbb{N}$.

a) $(a + b)\ mod\ n = (a\ mod\ n) + (b\ mod\ n)\ mod\ n$.

b) $a^d\ mod\ n = (a^{d-x} \cdot a^x)\ mod\ n = ((a^{d-x}\ mod\ n) \cdot (a^x\ mod\ n))\ mod\ n$. Für $x \leq d$.

c) Aus $a \equiv b \ (\ mod\ n)$ folgt $ac \equiv bc \ (\ mod\ n)$.

d) Aus $ac \equiv bc \ (\ mod\ n)$ folgt $a \equiv b \ (\ mod\ n)$. Für $c \neq 0 \ (\ mod\ n)$.

Aufgabe 3 (2 Punkte) ISBN-10. Geben Sie für jede Rechnung den Rechenweg mit an.

a) Zeigen oder widerlegen Sie: `386 883 091 X` ist eine gültige ISBN-10.

b) Zeigen oder widerlegen Sie: `558 488 508 4` ist eine gültige ISBN-10.

c) Zeigen Sie, dass `382 712 005 2` eine ungültige ISBN-10 ist. Wandeln Sie diese in eine gültige ISBN um (ohne die Prüfziffer zu ändern) und manipulieren Sie anschließend zwei Ziffern dieser gültigen ISBN, um eine neue gültige ISBN-10 zu erzeugen, die die gleiche Prüfziffer hat.

Aufgabe 4 (2 Punkte) GTIN 13. Geben Sie für jede Rechnung den Rechenweg mit an.

a) Zeigen oder widerlegen Sie: `978 158 488 508 5` ist eine gültige GTIN 13.

b) Zeigen oder widerlegen Sie: `978 061 800 125 2` ist eine gültige GTIN 13.

c) Zeigen Sie, dass `978 141 044 522 3` eine gültige GTIN 13 ist. Manipulieren Sie drei Ziffern, so dass diese GTIN 13 mit der neuen Prüfziffer 8 gültig ist.

Aufgabe 5 (2 Punkte) Programmieraufgabe Schreiben Sie ein Programm in Python, welches eine **ISBN-10** entgegennehmen kann und überprüft, ob die eingegebene Zahl gültig ist. Die zu überprüfende Nummer soll dabei als Kommandozeilenparameter übergeben werden können.

Beispiel: `./check_isbn.py 1805093079` liefert als output: `ungueltige ISBN-10`.
Beispiel: `./check_isbn.py 3938484217` liefert als output: `gueltige ISBN-10`.

Aufgabe 6 (2 Punkte) Programmieraufgabe Implementieren Sie den `Square-And-Multiply` Algorithmus aus der Vorlesung in Python. Das Programm soll dabei drei Zahlen x, y, n als Kommandozeilenparameter entgegennehmen und

$$result = x^y \ mod \ n$$

nach dem `Square-And-Multiply`-Prinzip berechnen. Der erste Parameter entspricht x, der zweite Parameter y und der letzte entspricht n. **Die Python-Funktion `pow()` darf lediglich für das Quadrieren einer Zahl verwendet werden!**

Beispiel 1: `./square_and_multiply.py 3 201 11` liefert als output: `3`.
Beispiel 2: `./square_and_multiply.py 123456789 9876 17` liefert als output: `1`.

Hinweis: Invalide Eingaben (zu lange, zu kurze oder fehlerhafte Zeichenketten) sollen behandelt werden und das Programm mit einer sinnvollen Fehlermeldung beendet werden.

Den Sourcecode als .py-Datei an `jakob.wenzel@uni-weimar.de`.