Universität Bielefeld **Wintersemester 2013/14**
C. Huck

Präsenzübungen zur Vorlesung

Diskrete Mathematik

Blatt 13

Aufgabe 1
Seit 1970 hat praktisch jedes kommerziell publizierte Buch eine Internationale Standard-Buch-Nummer (ISBN). Seit 2007 ist diese 13-stellig, vorher war sie 10-stellig. Für die 10-stellige ISBN $a_1a_2a_3a_4a_5a_6a_7a_8a_9a_{10}$ gilt folgende Regel: Die erste Ziffer a_1 bezeichnet die Sprache (0,1: Englisch, 2: Französisch, 3: Deutsch usw., 8,9: andere Sprachen, z.B. 88: Italienisch). Die nächsten Ziffern bezeichnen den Verlag, die dahinter den Titel. Die letzte Ziffer a_{10} ist eine Prüfziffer zwischen 0 und 10 (für 10 wird X verwendet). Diese Prüfziffer ist die (eindeutige!) Zahl mit

$$10a_1 + 9a_2 + 8a_3 + 7a_4 + 6a_5 + 5a_6 + 4a_7 + 3a_8 + 2a_9 + a_{10} \equiv 0 \mod 11$$

Die Prüfziffer kann die zwei häufigsten Tippfehler aufdecken: Genau eine Ziffer ist falsch, bzw. zwei aufeinanderfolgende Ziffern sind vertauscht.
Bestimmen Sie die fehlende Prüfziffer für die ISBN 3-8348-0084-?, sowie die fehlende Ziffer in der ISBN 3-41?-14842-X.
Welche der beiden: 3-525-82116-6 und 0-19-852058-3 ist als ISBN möglich, welche nicht? Zu der unmöglichen: Mittels der Zusatzinformation, dass lediglich zwei aufeinanderfolgende Ziffern vertauscht sind, ermitteln Sie die korrekte ISBN.

Aufgabe 2
Zeigen Sie, dass für jede Permutation $\pi \in S_n$ gilt:

$$\pi^{n!} = \mathrm{id}\,.$$

Aufgabe 3
Eine affine Cäsar-Verschlüsselung auf 26 Buchstaben ist von der Form $c\colon \mathbb{Z}_{26} \to \mathbb{Z}_{26}$, wobei $c([x]_{26}) := [ax + b]_{26}$ mit $0 < a, b < 26$. Zeigen Sie, dass c genau dann eine Bijektion ist, wenn $\mathrm{ggT}(a, 26) = 1$ gilt. Wieviele verschiedene solche Systeme gibt es also und wie sieht die Entschlüsselungsabbildung c^{-1} aus?

Aufgabe 4
(a) Verwenden Sie ein affines Cäsar-System auf 26 Buchstaben, um eine Botschaft zu verschlüsseln. Geben Sie anschließend Ihrem Sitznachbarn die Parameter a, b und überlassen sie Ihm die Entschlüsselung. Kehren Sie anschließend die Rollen um und verwenden Sie dabei evtl. ein anderes Cäsar-System auf 26 Buchstaben.

(b) Die folgende Nachricht wurde mit einem affinen Cäsar-System auf 26 Buchstaben verschlüsselt. Man entschlüssele $VBEDXSXIXKPXS$.

Hinweis. Für Teil (b) benötigt man natürlich einen Computer.

Aufgabe 5

Verwenden Sie das RSA-Verfahren mit dem öffentlichen Schlüssel $n = pq = 77$, $k = 7$, um Ihrem Sitznachbarn eine Botschaft zukommen zu lassen (offenbar müssen Sie jedes Zeichen einzeln verschlüsseln). Überlassen Sie die Bestimmung von p, q, m und natürlich die Entschlüsselung der Botschaft Ihm. Kehren Sie anschließend die Rollen um und verwenden Sie dabei evtl. einen neuen öffentlichen Schlüssel.

Hinweis. Wie üblich bedeutet 01: A, 02: B, ..., 26: Z, 00: Leerzeichen.