UNIVERSITÄT DES SAARLANDES
Fachrichtung 6.1 (Mathematik)
Prof. Dr. Mark Groves
MSc Jens Horn

Mathematik für Informatiker 1, WS 2018/19
Übungsblatt 6

---

1. Bobs public key lautet (in der Notation der Vorlesung)

$$n = 391, \qquad d = 13.$$

(a) Eve konnte jedoch seinen private key leicht bestimmen. Wie lautet er?

(b) Welches Wort hat Alice durch die Nachricht

$$172, 260, 260, 192, 43, 260, 334, 68$$

an Bob geschickt?

(c) Durch welche Nachricht würde Alice das Wort 'INFORMATIK' an Bob schicken?

[Sie sollen alle Schritte in Ihren Rechnungen angeben. Potenzieren lässt sich in modularer Arithmetik effizient durch 'quadrieren und multiplizieren' durchführen. Es gilt bspw.

$$\begin{aligned} 106 &\equiv 106 \pmod{143} \\ 106^2 \equiv 11236 &\equiv 82 \pmod{143} \\ 106^4 \equiv (82)^2 \equiv 6724 &\equiv 3 \pmod{143} \\ 106^8 \equiv (3)^2 \equiv 9 &\equiv 9 \pmod{143} \end{aligned}$$

und folglich

$$106^{11} \equiv (106)^8(106)^2 106 \equiv 9.82.106 \equiv 78227 \equiv 7 \pmod{143}. \ ]$$

2. Beweisen Sie die folgenden Aussagen durch vollständige Induktion:

(a) $\displaystyle\sum_{i=1}^{n} \log\left(1 + \frac{1}{i}\right) = \log(1+n)$ für jede natürliche Zahl n;

(b) $\displaystyle\prod_{i=1}^{n}(2i-1) = \frac{(2n)!}{2^n n!}$ für jede natürliche Zahl n;

(c) $n^2 \leq 2^n \leq n!$ für jede natürliche Zahl $n \geq 4$;

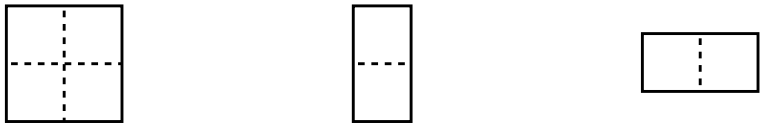
(d) $6|(2^n + 3^n - 5^n)$ für jede natürliche Zahl n.

3. (a) Es sei $\mathcal{P}(n)$, $n \in \mathbb{N}$ eine Aussageform mit den folgenden Eigenschaften:

- Es existiert $m \in \mathbb{N}$, so dass $\mathcal{P}(1)$, ..., $\mathcal{P}(m)$ wahr sind.
- Es sei $k > m$. Ist $\mathcal{P}(j)$ für alle $j < k$ wahr, so ist $P(k)$ wahr.

Folgern Sie aus dem Wohlordnungsaxiom der natürlichen Zahlen, dass $P(n)$ für alle $n \in \mathbb{N}$ wahr ist. (Dies ist das *Prinzip der starken vollständigen Induktion*).

(b) Im Spiel 'Mini-Tetris' geht es darum, ein $2 \times n$ Rechteck mit den folgenden Bausteinen lückenlos und ohne Überlappungen zu belegen:



Es sei T_n die Anzahl der verschiedenen Möglichkeiten, mit diesen Bausteinen ein $2 \times n$ Rechteck so zu belegen.

Bestimmen Sie T_1 und T_2, finden Sie eine Formel für T_n für $n \geq 3$ als Funktion von T_{n-1} und T_{n-2}, und beweisen Sie durch starke Induktion, dass

$$T_n = \frac{1}{3}[2^{n+1} + (-1)^n]$$

ist.