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

Mathematik für Informatiker 1, WS 2017/18
Übungsblatt 6

---

1. Bestimmen Sie das Infimum und das Supremum der Mengen

$$M_0 = \left\{ x \in \mathbb{Q} \ : \ \sqrt{3} < x \leq \sqrt{5} \right\},$$
$$M_1 = \left\{ \frac{1}{m} + \frac{1}{n} \ : \ m, n \in \mathbb{Z} \setminus \{0\} \right\},$$
$$M_2 = \left\{ \frac{x}{x+1} \ : \ x \in \mathbb{R},\ x > 0 \right\},$$
$$M_3 = \left\{ \frac{x+1}{x} \ : \ x \in \mathbb{R},\ x > 0 \right\}.$$

und entscheiden Sie, ob es sich hierbei um ein Minimum bzw. Maximum handelt.

2. Es seien A, B nichtleere, nichtdisjunkte Teilmengen des $\mathbb{R}$, die nach oben beschränkt sind. Beweisen Sie, dass $\sup A \cup B = \max\{\sup A, \sup B\}$ und $\sup A \cap B \leq \min\{\sup A, \sup B\}$. Geben Sie Teilmengen A, B von $\mathbb{R}$ mit der Eigenschaft $\sup A \cap B < \min\{\sup A, \sup B\}$ an.

3. (a) Zeigen Sie mithilfe des kleinen Satzes von Fermat, dass 63 und 341 keine Primzahlen sind. [Hinweis: Es ist $62 = 6.10 + 2$, $340 = 3.113 + 1$ und

$$1 \equiv 2^6 (\text{mod } 63), \qquad 1 \equiv 56^3 (\text{mod } 341).]$$

(b) Zeigen Sie mithilfe des kleinen Satzes von Fermat, dass 541 und 32769 keine Primzahlen sind.

(c) Sei nun p eine Primzahl. Zeigen Sie mithilfe des kleinen Satzes von Fermat, dass

$$(a+b)^p \equiv (a^p + b^p) \ (\text{mod } p)$$

gilt.

(d) Berechnen Sie

$$(3743^{3709} + 7420^{11127})^{3709} \ (\text{mod } 3709).$$

[Hinweis: 3709 ist eine Primzahl.]

4. 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

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