SAARLAND UNIVERSITY
Department of Mathematics
Prof. Dr. Mark Groves
MSc Jens Horn

Mathematics for Computer Scientists 1, WS 2017/18
Sheet 6

---

1. Determine the infima and suprema of the sets

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

and decide whether their minima and maxima exist.

2. Let A and B be nonempty, disjoint subsets of $\mathbb{R}$ which are bounded above. Prove that $\sup A \cup B = \max\{\sup A, \sup B\}$ and $\sup A \cap B \leq \min\{\sup A, \sup B\}$. Give an example of subsets A and B of $\mathbb{R}$ with the property that $\sup A \cap B < \min\{\sup A, \sup B\}$ an.

3. (a) Show using Fermat's little theorem that 63 and 341 are not prime numbers.
[Hint: $62 = 6.10 + 2$, $340 = 3.113 + 1$ and

$$1 \equiv 2^6 \pmod{63}, \qquad 1 \equiv 56^3 \pmod{341}.]$$

(b) Show using Fermat's little theorem that 541 and 32769 are not prime numbers.

(c) Let p be a prime number. Show using Fermat's little theorem that

$$(a+b)^p \equiv (a^p + b^p) \pmod{p}.$$

(d) Compute

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

[Hint: 3709 is a prime number.]

4. Bob's public key is (in the notation used in lectures)

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

(a) Eve was however easily able to determine his private key. What is it?

(b) Which word did Alice send to Bob via the message

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

(c) Which message would Alice use to send the word 'INFORMATIK' to Bob?

[You should give all the steps in your calculations. Powers may be efficiently calculated in modular arithmetic using the 'square and multiply' procedure. For example:

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

so that

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