Hochschule RheinMain
Prof. Dr. Steffen Reith

11. Übungsblatt

1. Sei $p = 11$, $q = 17$ und $e = 3$. Berechnen Sie den geheimen RSA-Schlüssel d und verschlüsseln Sie die Nachricht 5. Überprüfen Sie die Richtigkeit Ihres Ergebnisses indem Sie die verschlüsselte Nachricht auch wieder entschlüsseln.

2. Beweisen oder widerlegen Sie die folgenden Aussagen:

   i) $2n \in \mathcal{O}(n)$

   ii) $n^2 \in \mathcal{O}(n)$

   iii) $\log_2(n) \in \mathcal{O}(\log_k(n))$ für alle festen $k \in \mathbb{N}\backslash\{0,1\}$

   iv) $n^2 \in \mathcal{O}(n \cdot \log(n))$

   v) $n \cdot \log_2(n) \in \mathcal{O}(n^2)$

   vi) $3^n \in 2^{\mathcal{O}(n)}$

   a) $(2^n)^3 \in 2^{\mathcal{O}(n)}$

   b) $2^{n^3} \in 2^{\mathcal{O}(n)}$

   c) $\mathcal{O}(2^n) = \mathcal{O}(3^n)$

   d) $\mathcal{O}(2^{2n}) = \mathcal{O}(2^n)$

   e) $\mathcal{O}(n^2) + \mathcal{O}(n) = \mathcal{O}(n^2)$

   f) $\mathcal{O}(n) - \mathcal{O}(n) = \mathcal{O}(0)$

   Verwenden Sie die Tatsache, dass $f(n) \in \mathcal{O}(g(n))$, gdw. $c, n_0 \in \mathbb{N}$ gibt, so dass $\forall n \geq n_0$ gilt $f(n) \leq c \cdot g(n)$.

3. Beweisen oder widerlegen Sie die folgenden Aussagen:

   i) $n \in \mathrm{o}(2n)$

   ii) $2n \in \mathrm{o}(n^2)$

   iii) $n^k \in \mathrm{o}(2^n)$ für alle festen $k \in \mathbb{N}$

   iv) $2^n \in \mathrm{o}(3^n)$

   v) $1 \in \mathrm{o}(n)$

   a) $1 \in \mathrm{o}(\frac{1}{n})$

   b) $\log_2(n) \in \mathrm{o}(n)$

   c) $n^2 \in \mathrm{o}(\log_2(n))$

   d) $\mathrm{o}(g(n)) \subseteq \mathcal{O}(g(n))$ für alle Funktionen $g : \mathbb{N} \to \mathbb{N}$

   Verwenden Sie die Tatsache, dass $f \in \mathrm{o}(g)$, gdw. $\forall c > 0\ \exists n_0\ \forall n > n_0$ so, dass $f(n) < c \cdot g(n)$.

4. Zeigen Sie, dass $3^n \notin O(2^n)$, $5n + 2 \in o(n^2)$ und $n \in o(n^2)$

5. Sei $q(x) = a_m x^m + a_{m-1} x^{m-1} + \ldots + a_1 x + a_0$ mit $a_i \in \mathbb{Z}$ für $0 \leq i \leq m$ ein beliebiges Polynom. Beweisen Sie, dass x^m eine *dichte asymptotische Schranke* für q ist.

6. Seien $f, g \colon \mathbb{N} \to \mathbb{N}$ mit $O(g) = O(f)$. Gilt dann auch $g = f$? Ist dies der Fall, so beweisen Sie dies. Im anderen Fall geben Sie ein geeignetes Gegenbeispiel.

Besprechung in der Übung am 24. Januar 2018