Einführung in das symbolische Rechnen
Übungsblatt 4

Abgabe bis Montag, den 14.05.2018, 14:00 im Abgabekasten.

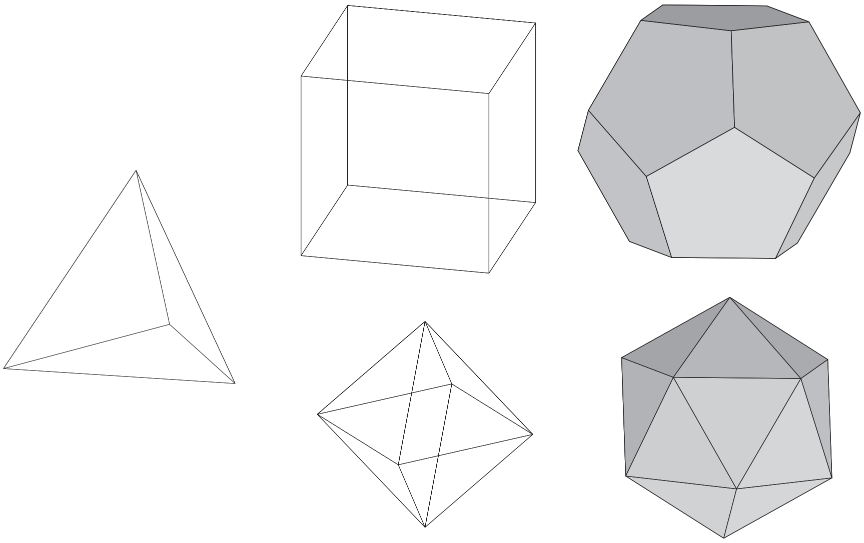
1. Sei x in einem kommutativen Ring R mit 1 und $n \in \mathbb{N}$.

   (a) Beschreiben Sie ein Verfahren, das mittels iterativem Quadrieren x^n berechnet.

   (b) Bestimmen Sie die Anzahl der R-Multiplikationen Ihres Verfahrens in Landau-Notation abhängig von n.

   (c) Wenden Sie das Verfahren an, um 3^{11} in $\mathbb{Z}$ und $\overline{3}^{11}$ in $\mathbb{Z}/7$ zu berechnen.

2. Basteln Sie Papiermodelle der Platonischen Körper Tetraeder, Würfel, Oktaeder, Dodekaeder und Ikosaeder. Bitte in die Übung mitbringen.



3. Finden Sie für alle Platonischen Körper jeweils eine Drehsymmetrie und eine Spiegelsymmetrie und beschreiben Sie diese als Elemente der symmetrischen Gruppe S_n mit n die Anzahl der Ecken des Platonischen Körpers.

4. Sei $B \in \mathbb{Z}$, $B \geq 2$ und seien zwei Zahlen

$$x = \sum_{i=0}^{m-1} a_i B^i \qquad y = \sum_{i=0}^{n-1} b_i B^i$$

   in B-adischer Entwicklung zur Basis B mit $a_{m-1}, b_{n-1} \neq 0$ und

$$1 < \frac{x}{y} < B$$

   gegeben. Sei weiter $x = q \cdot y + r$ mit $0 \leq r < y$ das Resultat der Division mit Rest von x durch y. Wir definieren $\widetilde{q}$ als das Minimum von $B - 1$ und

$$\left\lfloor \frac{a_n \cdot B + a_{n-1}}{b_{n-1}} \right\rfloor$$

   (a) Bestimmen Sie q und $\widetilde{q}$ für $B = 10$ und

$$x = 3142351 \qquad y = 677688.$$

(b) Zeigen Sie allgemein: Ist

$$b_{n-1} \geq \left\lfloor \frac{B}{2} \right\rfloor$$

dann gilt

$$q \leq \widetilde{q}.$$

5. (4 Zusatzpunkte)

(a) Zeigen Sie, dass mit der Notation von Aufgabe 4 auch gilt

$$\widetilde{q} \leq q + 2$$

(b) Folgern Sie, dass unter den Voraussetzung von Aufgabe 4 bei der Division mit Rest die Zahl q in höchstens $3 \in O(1)$ Versuchen gefunden werden kann.