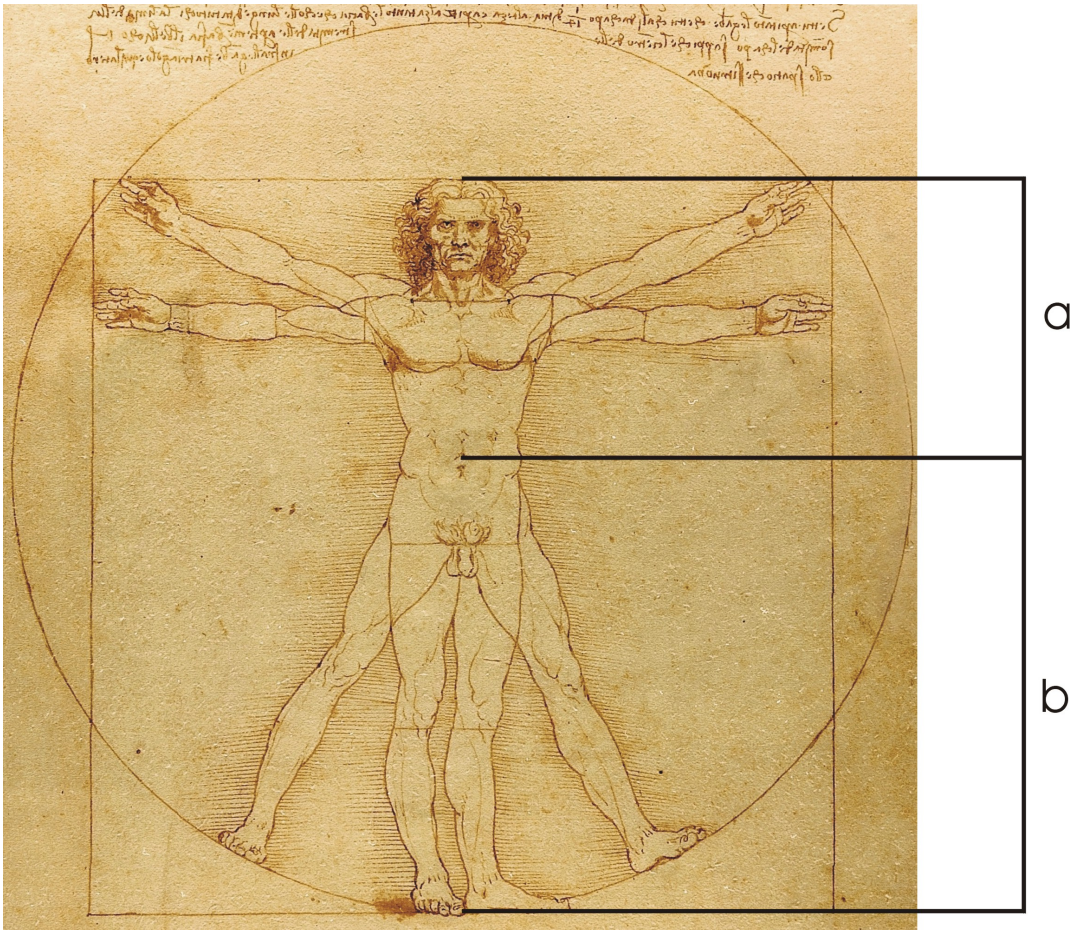
Einführung in das symbolische Rechnen
Übungsblatt 11

Abgabe bis Montag, den 09.07.2018, 14:00 im Abgabekasten.

1. Leonardo da Vinci hat vermutet, dass das Längenverhältnis $\frac{b}{a}$ in der folgenden Abbildung eine algebraische Zahl $r \in \overline{\mathbb{Q}}$ ist.



   (a) Messen Sie a und b so genau wie möglich ab, und berechnen Sie numerisch eine Näherung für $\frac{b}{a}$.

   (b) Bestimmen Sie mit Hilfe des LLL-Algorithmus aus der Näherung einen Kandidaten für r.

   (c) Erproben Sie das Verfahren auch an Ihren eigenen Maßen.

2. Berechnen Sie eine LLL-reduzierte Basis des Gitters L erzeugt von den Vektoren

$$\begin{pmatrix} 4 \\ 4 \\ 6 \end{pmatrix}, \begin{pmatrix} 5 \\ 8 \\ 2 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \\ 6 \end{pmatrix} \in \mathbb{Z}^3$$

   Folgen Sie dabei dem Algorithmus Schritt für Schritt.

3. Sei $L \subset \mathbb{R}^n$ ein Gitter von Rang n und $(v_1, ..., v_n)$ eine $\delta - LLL$-reduzierte Basis von L. Seien weiter $y_1, ..., y_l$ linear unabhängige Vektoren in L. Zeigen Sie, dass mit

$$\tau = \frac{4}{4\delta - 1}$$

   gilt

$$\|v_j\| \leq \tau^{\frac{n-1}{2}} \cdot \max\{\|y_1\|, ..., \|y_l\|\}$$

   für alle $j = 1, ..., l$.

4. Sei R ein kommutativer Ring mit 1. Zeigen Sie, dass für die formale Ableitung

$$(-)' : R[x] \to R[x],\ \textstyle\sum_{i=0}^{d} a_i x^i \mapsto \sum_{i=0}^{d} i a_i x^{i-1}$$

gilt $f' = 0$ für $f \in R$ und

$$\begin{aligned}(f+g)' &= f' + g' \\ (f \cdot g)' &= f' \cdot g + f \cdot g' \\ (f^n)' &= n \cdot f^{n-1} \cdot f'\end{aligned}$$

für alle $f, g \in R[x]$, $n \in \mathbb{N}$.

5. (4 Zusatzpunkte) Sei p eine Primzahl, $\mathbb{F}_p = \mathbb{Z}/p = \{\overline{0}, ..., \overline{p-1}\}$ der Körper mit p Elementen und $f \in \mathbb{F}_p[x_1, ..., x_n]$ ein nicht-konstantes Polynom. Die Anzahl der möglichen Werte $f(x)$, die f für jeden Punkt $x \in \mathbb{F}_p^n$ annehmen kann, ist $|\mathbb{F}_p| = p$. Setzen Sie voraus, dass f für zufällig gewähltes x alle diese Werte mit gleicher Wahrscheinlichkeit $\frac{1}{p}$ annimmt.

   (a) Wie hoch ist die Wahrscheinlichkeit, dass $f(x) = 0$ für zufälliges x, falls f das Produkt von zwei irreduziblen Polynomen ist.

   (b) Entwickeln Sie ein Verfahren, das Irreduzibilität probabilistisch testet.

   Hinweis: Betrachten Sie die relative Häufigkeit der Nullstellen von f für eine Stichprobe aus $N \geq 0$ zufällig gewählten Punkten $x \in \mathbb{F}_p^n$.

   (c) Erproben Sie Ihre Methode an einfachen Beispielen und vergleichen Sie mit dem SINGULAR-Kommando `factorize`.