Einführung in das symbolische Rechnen
Übungsblatt 11

Abgabe Mittwoch, den 14.07.2021 bis 23:59 in OpenOlat.

1. Sei

$$A = \begin{pmatrix} 2 & 2 & 2 & 2 \\ 3 & 3 & 3 & 3 \\ 2 & 4 & 6 & 2 \\ 3 & 3 & 6 & 3 \end{pmatrix} \in \mathbb{Z}^{4\times 4}$$

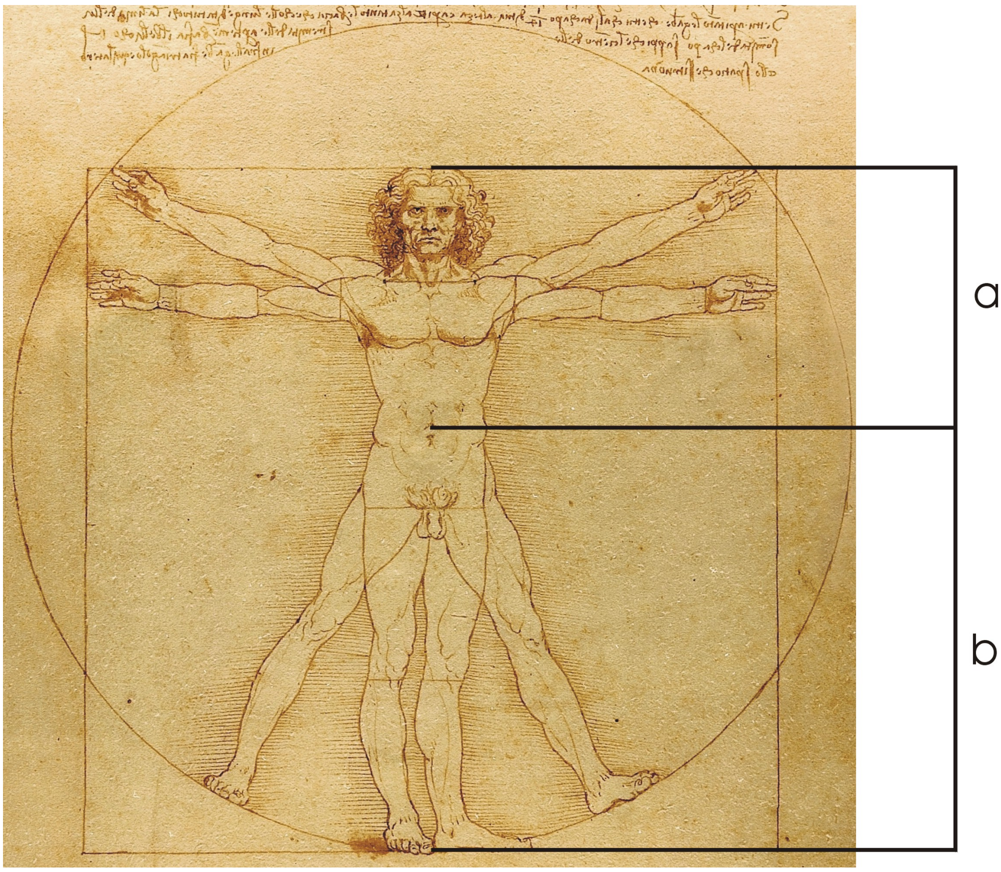
   Bestimmen Sie

   (a) die Hermite-Normalform D von A und $T \in \mathrm{GL}(4,\mathbb{Z})$ mit

   $$A \cdot T = D,$$

   (b) und daraus eine Basis des Bilds und des Kerns von A.

2. 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 aus der Näherung einen Kandidaten für r.

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

3. Seien $p_1 = 101$ und $p_2 = 103$ und
$$\frac{a}{b} \in \mathbb{Q}$$
mit $p_i \nmid b \ \forall i$ und $a^2 + b^2 < N = p_1 \cdot p_2$. Modulo p_1 und p_2 wurde $\overline{x} = \overline{a} \cdot \overline{b}^{-1}$ berechnet als
$$\overline{x} = \overline{79} \in \mathbb{Z}/p_1$$
$$\overline{x} = \overline{27} \in \mathbb{Z}/p_2$$

   (a) Bestimmen Sie mit dem Chinesischen Restsatz $r \in \mathbb{Z}$ mit $0 \leq r < N$ und
$$r \equiv 79 \bmod p_1$$
$$r \equiv 27 \bmod p_2$$

   (b) Bestimmen Sie a und b aus r, indem Sie in dem Gitter der $\mathbb{Z}$-Linearkombinationen von
$$\begin{pmatrix} N \\ 0 \end{pmatrix}, \begin{pmatrix} r \\ 1 \end{pmatrix}$$
einen kürzesten Vektor finden.

   (c) Überprüfen Sie, dass Ihr Resultat die obigen Kongruenzen erfüllt.

4. Sei $L \subset \mathbb{R}^2$ ein Gitter mit Basis (v_1, v_2). Der Gauß-Lagrange-Algorithmus funktioniert wie folgt:

   1: **reduziere** v_2 nach v_1, d.h.
$$v_2 = v_2 - \left\lfloor \frac{\langle v_1, v_2 \rangle}{\|v_1\|^2} \right\rceil \cdot v_1$$
   2: **if** $\|v_2\| < \|v_1\|$ **then**
   3:     **vertausche** v_1 und v_2
   4:     **goto** 1
   5: **return** (v_1, v_2)

   Zeigen Sie:

   (a) Dieser Algorithmus terminiert.

   (b) In der vom Gauß-Lagrange-Algorithmus berechneten Basis (v_1, v_2) ist der Vektor v_1 ein kürzester Vektor in L, d.h.
$$\|v\| \geq \|v_1\|$$
für alle $v \in L$.

   (c) Wenden Sie den Gauß-Lagrange-Algorithmus an auf das Gitter L erzeugt von
$$v_1 = \begin{pmatrix} 101 \\ 0 \end{pmatrix} \qquad v_2 = \begin{pmatrix} 68 \\ 1 \end{pmatrix}$$

5. (4 Zusatzpunkte) 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
$$(f+g)' = f' + g'$$
$$(f \cdot g)' = f' \cdot g + f \cdot g'$$
$$(f^n)' = n \cdot f^{n-1} \cdot f'$$
für alle $f, g \in R[x]$, $n \in \mathbb{N}$.