Seminar: Computeralgebra 1
Thema 6 : Modulare Determinatenberechnung
Tobias Kreisel

0.1 Der chinesische Restsatz

Satz 1

Seien R ein euklidischer Bereich, $m_0, \ldots, m_{r-1}$ paarweise teilerfremd (also insbesondere $\text{ggT}(m_i, m_j) = 1\ \forall i \neq j$).
Definiere Ringhomomorphismus:

$$\pi_i : R \longrightarrow R/(m_i), \quad f \longmapsto f \text{ mod } m_i.$$

Kombiniert für alle i ergibt dies:

$$\begin{aligned} \chi = \pi_0 \times \cdots \times \pi_{r-1} : R \longrightarrow & R/(m_0) \times \cdots \times R/(m_{r-1}), \\ f \longmapsto & (f \text{ mod } m_0, \ldots, f \text{ mod } m_{r-1}). \end{aligned}$$

Behauptung: χ ist surjektiv mit $\text{Kern}(\chi) = (m)$, wobei $m := m_0 \cdot \ldots \cdot m_{r-1}$.

Beweis
Kern:

$$\begin{aligned} \text{Sei} f \in Kern(\chi) &\iff \chi(f) = (f \text{ mod } m_0, \ldots, f \text{ mod } m_{r-1}) = (0, \ldots, 0) \\ &\iff m_i \mid f\ \forall i : 0 \leq i < r \\ &\iff m \mid f \Rightarrow Kern(\chi) = (m). \end{aligned}$$

Surjektivität:
Zeige: Es existiert $l_i \in R$ mit $\chi(l_i) = e_i$ $(0 \leq i < r)$, wobei $e_i = (0, \ldots, 0, 1, 0, \ldots, 0) \in R/(m_0) \times \cdots \times R/(m_{r-1})$.
Dies genügt, da: Sei $v = (v_0 \text{ mod } m_0, \ldots, v_{r-1} \text{ mod } m_{r-1}) \in R/(m_0) \times \cdots \times R/(m_{r-1})$ beliebig, $v_0, \ldots, v_{r-1} \in R$. Dann gilt:

$$\begin{aligned} \chi(\sum_{i=0}^{r-1} v_i l_i) = \sum_{i=0}^{r-1} \chi(v_i)\chi(l_i) &= \sum_{i=0}^{r-1} (v_i \text{ mod } m_0, \ldots, v_i \text{ mod } m_{r-1}) \cdot e_i \\ &= \sum_{i=0}^{r-1} (0, \ldots, 0, v_i \text{ mod } m_i, 0, \ldots, 0) = v \end{aligned}$$

<u>oBdA $i = 0$:</u>
Der erweiterte euklidische Algorithmus (EEA) angewandt auf $m_1 \cdot \ldots \cdot m_{r-1} = \frac{m}{m_0}$ und m_0 liefert $s, t \in R$ mit $s \cdot \frac{m}{m_0} + t \cdot m_0 = 1$ (möglich, da m_i teilerfremd).
Setze also $l_0 = s \cdot \frac{m}{m_0}$, dieses hat gewünschte Eigenschaft:

$$\begin{aligned} l_0 = s \cdot \frac{m}{m_0} \equiv s \cdot \frac{m}{m_0} + t \cdot m_0 \equiv & 1 \pmod{m_0} \\ \equiv & 0 \pmod{m_j}\ (j = 1, \ldots, r-1). \end{aligned}$$

Somit folgt: $\chi(l_0) = e_0$. $\square$

0.1.1 Folgerung:

Da wir den Kern von χ kennen, können wir folgenden Ringisomorphismus definieren:

$$\begin{aligned} \tilde{\chi} : R/(m) &\longrightarrow R/(m_0) \times \cdots \times R/(m_{r-1}), \\ f \bmod m &\longmapsto (f \bmod m_0, \ldots, f \bmod m_{r-1}) \end{aligned}$$

0.2 Algorithmus chinese1

<u>input:</u> $m_0, \ldots, m_{r-1} \in R$ paarw. teilerfremd $v_0, \ldots, v_{r-1} \in R$
<u>output:</u> $f \in R$ mit $f \equiv v_i \pmod{m}_i$ $(0 \leq i < r)$
Schritt 1: $m \longleftarrow m_0 \cdot \ldots \cdot m_{r-1}$
Schritt 2: Berechne $s_i, t_i \in R$ mit

$$\begin{aligned} s_i \cdot \frac{m}{m_i} + t_i \cdot m_i = 1 \quad &\text{(EEA)} \\ c_i \longleftarrow v_i \cdot s_i \bmod m_i & \end{aligned}$$

Schritt 3: Ausgabe von $\sum_{i=0}^{r-1} c_i \cdot \frac{m}{m_i}$

Da obenstehender Algorithmus auf die explizite Berechnung von $m := m_0 \cdot \ldots \cdot m_{r-1}$ angewiesen ist, erzeugt man unnötig große Werte. Deshalb konstruieren wir noch folgenden Algorithmus.

0.3 Algorithmus chinese2

<u>input/output:</u> siehe chinese1
Schritt 0: Setze $f_0 := v_0$ $\quad n_0 := m_0$
Schritt i: Fuer $i = 1, \ldots, r-1$ berechne $a \cdot n_{i-1} + b \cdot m_i = 1$. Setze:

$$\begin{aligned} z &:= (v_i - f_{i-1}) \cdot a \pmod{m_i} \\ f_i &:= f_{i-1} + z \cdot n_{i-1} \\ n_i &:= n_{i-1} \cdot m_i \end{aligned}$$

Beweis (per Induktion)
<u>$i = 0:$</u> $f_0 \equiv v_0 \bmod m_0$ $\quad\checkmark$
<u>$i - 1 \rightarrow i:$</u> Zeige
  a) fuer $j = i:$ $f_i \equiv v_i \pmod{m_i}$
  b) fuer $j < i:$ $f_i \equiv v_j \pmod{m_j}$
zu a) Es gilt: $a \cdot n_{i-1} + b \cdot m_i = 1 \Rightarrow a \cdot n_{i-1} \equiv 1 \pmod{m_i}$
  $\Longrightarrow z \cdot n_{i-1} = (v_i - f_{i-1}) \cdot a \cdot n_{i-1}$
  $\Longrightarrow f_i = f_{i-1} + z \cdot n_{i-1} \equiv f_{i-1} + v_i - f_{i-1} \equiv v_i \pmod{m_i}$
zu b) Es gilt: $n_{i-1} = m_0 \cdot \ldots \cdot m_{i-1} \equiv 0 \pmod{m_j}$

$$\Longrightarrow f_i = f_{i-1} + z \cdot n_{i-1} \equiv f_{i-1} \pmod{m_j} \equiv v_j \pmod{m_j}$$

$\square$

0.4 Algorithmus Modulare Determinatenberechnung

input: $A \in \mathbb{Z}^{n \times n}$, mit $|a_{ij}| \leq B \; \forall i, j$.
output: $\det(A) \in \mathbb{Z}$.
Schritt 1: $C \longleftarrow n^{\frac{n}{2}} \cdot B^n$ (Hadamard Abschaetzung der det nach oben)
Wähle r Primzahlen m_i, sodass: $\prod_{i=0}^{r-1} m_i > C$
Schritt 2: Berechne $\overline{A} \equiv A \pmod{m_i}$ fuer $i = 0, \ldots, r-1$.
Schritt 3: Berechne $v_i \in \{0, \ldots, m_{i-1}\}$, sodass $v_i \equiv \det(A) \pmod{m_i}$
Schritt 4: Berechne $d \equiv v_i \pmod{m_i}$ mit Hilfe von chinese1/2. Gebe d aus.