Algorithmische Methoden 1

Wolfgang Windsteiger

RISC Institut

Das Thema der heutigen Vorlesung

Die rationalen Zahlen $\mathbb{Q}$

$\mathbb{Q}$ als Erweiterung von $\mathbb{Z}$

- $\mathbb{Z}$ so erweitern, dass eine Division im Sinne der Umkehrung der Multiplikation möglich wird $\rightsquigarrow$ Invertieren bzgl. der Multiplikation.
- Bilden Paare von ganzen Zahlen.
- Manche Paare stehen für die gleiche Zahl $\rightsquigarrow$ identifiziere diese Paare $\rightsquigarrow$ Äquivalenzrelation:

$$(z, n) \sim (z', n') :\Leftrightarrow z \cdot n' = n \cdot z'.$$

Satz

Die Relation $\sim$ ist eine Äquivalenzrelation auf $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$.

Rechnen in $\mathbb{Q}$

- Die Äquivalenzklasse von (z, n) bezüglich $\sim$ wird als $\frac{z}{n}$ geschrieben. Jedes $\frac{z}{n}$ nennt man einen Bruch (über $\mathbb{Z}$), wobei z der Zähler und n der Nenner des Bruchs genannt wird.
- Rationale Zahlen:
$$\mathbb{Q} := \{\frac{z}{n} \mid z, n \in \mathbb{Z} \wedge n \neq 0\}.$$
- Rechnen:
$$\frac{z}{n} + \frac{z'}{n'} := \frac{z \cdot n' + z' \cdot n}{n \cdot n'} \qquad \frac{z}{n} \cdot \frac{z'}{n'} := \frac{z \cdot z'}{n \cdot n'}.$$
- Multiplikative Inverse und Division:
$$\left(\frac{z}{n}\right)^{-1} = \frac{n}{z}$$
$$\frac{z}{n} / \frac{z'}{n'} := \frac{z}{n} \cdot \frac{n'}{z'}$$

Darstellung am Computer

- Rechnen in $\mathbb{Q} \rightsquigarrow$ Rechnen mit Äquivalenzklassen.
- Analog zu $\mathbb{Z}_m$: Verwende Repräsentantensystem $R \rightsquigarrow$ Rechnen mit Paaren von ganzen Zahlen.
- Kanonischer Simplifikator

$$\text{kanonisch}_{\mathcal{Q}}((z,n)) := ((z \operatorname{div} t) \cdot \operatorname{sgn}(n), |n| \operatorname{div} t) \;\text{ mit } t = \operatorname{ggT}(z,n).$$

Computerrepräsentation (Datenstruktur $\mathcal{Q}$ für rationale Zahlen)

Datenstruktur $\mathcal{Q}$, in der Zähler und Nenner des kanonischen Repräsentanten einer Klasse abgespeichert sind. Zähler und Nenner von $a \in \mathcal{Q}$ sprechen wir durch $\textit{zähler}(a)$ und $\textit{nenner}(a)$ an.

Rechnen in $\mathbb{Q}$

$$
\begin{aligned}
(z,n) \pm (z',n') &:= \text{kanonisch}_{\mathbb{Q}}((z \cdot n' \pm z' \cdot n, n \cdot n')) \\
(z,n) \cdot (z',n') &:= \text{kanonisch}_{\mathbb{Q}}((z \cdot z', n \cdot n')) \\
(z,n)^{-1} &:= \text{kanonisch}_{\mathbb{Q}}((n,z)) \quad \text{für } z \neq 0 \\
(z,n) \,/\, (z',n') &:= (z,n) \cdot (n',z') \quad \text{für } z' \neq 0.
\end{aligned}
$$

Algorithmus *AddQ*: Addition in $\mathbb{Q}$

$z \leftarrow \mathit{zähler}(a)$, $n \leftarrow \mathit{nenner}(a)$
$z' \leftarrow \mathit{zähler}(b)$, $n' \leftarrow \mathit{nenner}(b)$
$(z,n) \leftarrow \text{kanonisch}_{\mathbb{Q}}((z \cdot n' + z' \cdot n, n \cdot n'))$
$\mathit{zähler}(s) \leftarrow z$, $\mathit{nenner}(s) \leftarrow n$
return s

Aufruf: $AddQ(a,b)$
Eingabe: $a, b \in \mathbb{Q}$
Ausgabe: $s \in \mathbb{Q}$
mit: $s = a + b$.

Henrici Algorithmus zur Addition

- Für kanonische Form der Summe: $\mathrm{ggT}(\underbrace{z \cdot n' + z' \cdot n}_{=u'}, \underbrace{n \cdot n'}_{=v'})$.
- $t = \mathrm{ggT}(n, n') \rightsquigarrow n = t \cdot N$ und $n' = t \cdot N'$.
- t ist ein gemeinsamer Teiler von u' und v'. Es verbleibt die Berechnung von $\mathrm{ggT}(z \cdot N' + z' \cdot N, n \cdot N')$.

Satz (Henrici Addition)

Seien $z, n, z', n' \in \mathbb{Z}$ mit $n, n' \neq 0$ und $\mathrm{ggT}(z, n) = \mathrm{ggT}(z', n') = 1$, und seien weiters $t = \mathrm{ggT}(n, n')$, $N = n \operatorname{div} t$ und $N' = n' \operatorname{div} t$. Dann ist

$$\mathrm{ggT}(z \cdot N' \pm z' \cdot N, n \cdot N') = \mathrm{ggT}(z \cdot N' \pm z' \cdot N, t).$$

Henrici Algorithmus zur Addition

Algorithmus *AddQHenrici*: Henrici Addition in $\mathbb{Q}$

$$
\begin{aligned}
&z \leftarrow \mathit{z\ddot{a}hler}(a),\ n \leftarrow \mathit{nenner}(a)\\
&z' \leftarrow \mathit{z\ddot{a}hler}(b),\ n' \leftarrow \mathit{nenner}(b)\\
&t \leftarrow \mathrm{ggT}(n, n'),\\
&N \leftarrow n \operatorname{div} t,\ N' \leftarrow n' \operatorname{div} t\\
&u \leftarrow z \cdot N' + z' N,\ v \leftarrow n \cdot N',\\
&t' \leftarrow \mathrm{ggT}(u, t)\\
&\mathit{z\ddot{a}hler}(s) \leftarrow u \operatorname{div} t'\\
&\mathit{nenner}(s) \leftarrow v \operatorname{div} t'\\
&\textbf{return } s
\end{aligned}
$$

Aufruf:	$\mathit{AddQHenrici}(a, b)$
Eingabe:	$a, b \in \mathbb{Q}$
Ausgabe:	$s \in \mathbb{Q}$
mit:	$s = a + b$.

Beispiel: $\rightsquigarrow$ *Mathematica*

Henrici Algorithmus zur Multiplikation

Satz (Henrici Multiplikation)

Seien $z, n, z', n' \in \mathbb{Z}$ *mit* $n, n' \neq 0$ *und* $\operatorname{ggT}(z, n) = \operatorname{ggT}(z', n') = 1$, *und seien* $t = \operatorname{ggT}(z, n')$, $t' = \operatorname{ggT}(z', n)$ *und* $Z = z \operatorname{div} t$, $N = n \operatorname{div} t'$, $Z' = z' \operatorname{div} t'$, $N' = n' \operatorname{div} t$. *Dann ist*

$$\operatorname{ggT}(Z \cdot Z', N \cdot N') = 1.$$

Henrici Algorithmus zur Multiplikation

Algorithmus *MultQHenrici*: Henrici Multiplikation in $\mathbb{Q}$

$$
\begin{aligned}
& z \leftarrow \mathit{z\ddot{a}hler}(a),\ n \leftarrow \mathit{nenner}(a) \\
& z' \leftarrow \mathit{z\ddot{a}hler}(b),\ n' \leftarrow \mathit{nenner}(b) \\
& t \leftarrow \mathrm{ggT}(z, n'),\ t' \leftarrow \mathrm{ggT}(z', n) \\
& Z \leftarrow z \operatorname{div} t,\ N \leftarrow n \operatorname{div} t' \\
& Z' \leftarrow z' \operatorname{div} t',\ N' \leftarrow n' \operatorname{div} t \\
& \mathit{z\ddot{a}hler}(p) \leftarrow Z \cdot Z' \\
& \mathit{nenner}(p) \leftarrow N \cdot N' \\
& \mathbf{return}\ p
\end{aligned}
$$

$$
\begin{aligned}
\text{Aufruf:}\ & \mathit{MultQHenrici}(a, b) \\
\text{Eingabe:}\ & a, b \in \mathbb{Q} \\
\text{Ausgabe:}\ & p \in \mathbb{Q} \\
\text{mit:}\ & p = a \cdot b.
\end{aligned}
$$

Beispiel: $\rightsquigarrow$ *Mathematica*