”Hallo Welt!” für Fortgeschrittene

Arithmetik und Algebra

von Gerhard Pfeiffer

(sigepfei@stud.informatik.uni-erlangen.de)

Seminarvortrag am 29. Juni 2004

Inhalt

- Arithmetik? Algebra? Was ist das überhaupt?
- Rechnen mit grossen Zahlen
- Chinesischer Restesatz
- Diophantische Gleichungen
- Gauß-Algorithmus

Arithmetik? Algebra? Was ist das überhaupt?

- Arithmetik
  [griech. ”Zahlenlehre”]
  Teilgebiet der Mathematik, das sich mit Zahlen und deren Rechenregeln beschäftigt.
- Algebra
  [arabisch]
  Gleichungslehre als Teilgebiet der Mathematik, Buchstabenrechnung, im modernen Sinne Lehre von den formalen Rechenbereichen (Ring, Körper u.ä.), Übernahme (Mitte 15. Jahrhundert) von gleichbedeutend lat. algebra, gebildet in Anlehnung an arab. al-gabr, eigentlich ”Wiederherstellung”.

Arithmetik

Rechnen mit grossen (Ganz-)Zahlen

- Darstellung von grossen Zahlen
  - Array
    Leicht zu implementieren
    Quasi statisch (`realloc`)
  - Verkettete Liste
    Dynamisch, schwieriger zu implementieren
    Mehr overhead durch Liste (next-Pointer)
- Prinzip:
  - Einzelne Ziffern (nicht zwingend Basis 10) als Array-/Listenelemente.
  - Rechnen wie in der Schule
  - Implementierungsbeispiel siehe Buch ”Programming Challenges”

Chinesischer Restesatz

Formosa's Soldiers (Problem E, Dezember-Contest)

- Die Bewohner der Insel Formosa leben in ständiger Angst vor einer feindlichen Invasion; deswegen wurde eine riesige Armee aufgestellt.
- Problem: Wieviele Soldaten sind angetreten?
- Lösungsvorschlag:
  Soldaten bilden Gruppen zu p Leuten. Gezählt wird, wieviele übrig bleiben. Dies wird mit unterschiedlichen Primzahlen p wiederholt.
  Aus den Resten lässt sich die komplette Anzahl an Soldaten konstruieren.
- In insider-Kreisen bekannt als: Formosa Theorem

Modulare Arithmetik

- Repräsentation einer Zahl durch Moduli.
- Vorausgesetzt, $x < m = \prod m_i$ und alle m_i paarweise teilerfremd, lässt sich x eindeutig darstellen durch ein Kongruenzensystem:

$$x_i \equiv x \pmod{m_i}$$

- Gäbe es ein $y < m$ mit gleicher Darstellung, so folgt $x = y$. Aufgrund der gleichen Darstellung gilt $(x - y) \equiv 0 \pmod{m_i}$ und damit auch $(x - y) \equiv 0 \pmod{m}$.
- Wie kommt man nun von der modularen Darstellung zur Zahl?

Modulare Arithmetik

- Wie kommt man von der modularen Darstellung zur Zahl?
- Finde für jedes Paar m_i, m_j ein a_{ij} mit $a_{ij} \cdot m_i \equiv 1 \bmod \mathrm{m_j}$. Dies geht über eeA / Bezout-Koeffizienten: $a_{ij} \cdot m_i + b \cdot m_j = 1$.
- Mit diesen a_{ij} lassen sich nun y_i bestimmen:

$$
\begin{aligned}
y_1 &\leftarrow x_1 \bmod \mathrm{m_1} && (1)\\
y_2 &\leftarrow (x_2 - y_1) \cdot a_{12} \bmod \mathrm{m_2} && (2)\\
y_3 &\leftarrow ((x_3 - y_1) \cdot a_{13} - y_2) \cdot a_{23} \bmod \mathrm{m_2} && (3)\\
&\vdots && (4)\\
y_n &\leftarrow (\ldots((x_n - y_1) \cdot a_{2n} - y_2) \cdot a_{2r} - && (5)\\
&\qquad \ldots - y_n - 1) \cdot a_{(n-1)n} \bmod \mathrm{m_n} && (6)
\end{aligned}
$$

- Und damit schliesslich x: $x = y_1 + y_2 m_1 + y_3 m_1 m_2 + \ldots$

Modulare Arithmetik

- Beispiel:
- $x \equiv 3 \bmod 5$ und $x \equiv 2 \bmod 7$
- Bezout-Koeffizienten für 5 und 7:

$$3 \cdot 5 - 2 \cdot 7 = 1$$

- Also: $3 \cdot 5 \equiv 1 \bmod 7$, $-2 \cdot 7 \equiv 1 \bmod 5$
- y_i bestimmen:

$$y_1 = 3$$

$$y_2 = (2 - 3) \cdot 3 \bmod 7 = 4$$

- x bestimmen:

$$x = 3 + 4 \cdot 5 = 23$$

Modulare Arithmetik

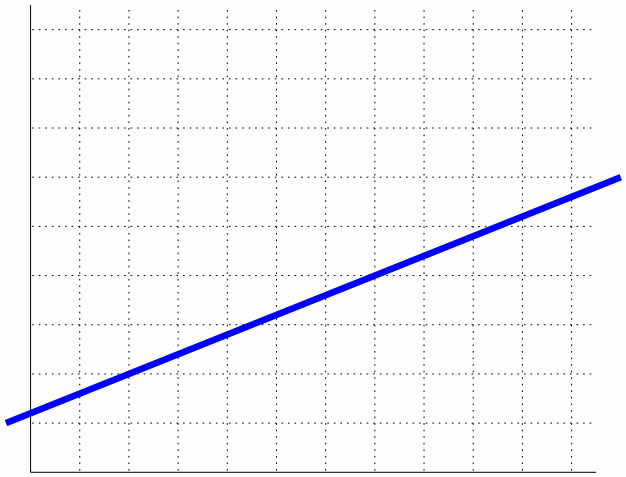
- Algorithmus:
  - Berechne y_i:

    $y_1 \leftarrow x_1$
    for $j \leftarrow 2$ to n:
      $y_j \leftarrow x_j - y_1$
      for $i \leftarrow 1$ to $j - 2$:
        $y \leftarrow y_j \cdot a_{ij}$
      $y_j \leftarrow y_j \cdot a_{j-1,j} \bmod \mathrm{m_j}$
  - Berechne x aus den y_i:

    $x \leftarrow y_1$
    for $j \leftarrow 2$ to n:
      $z \leftarrow y_j$
      for $i \leftarrow 1$ to $j - 1$:
        $z \leftarrow z \cdot m_i$
    $x \leftarrow z + x$

Diophantische Gleichungen

Schnittpunkte mit den Koordinatensystem



- $y = \frac{2}{5}x + 1\frac{1}{5}$
- Gesucht: ganzzahlige Lösungen von

$$5y - 2x = 6$$

Erweiterter Euklid liefert: $y = 6$, $x = 12$

Diophantische Gleichungen

- Definition:
  Gleichung(ssystem), für das nur ganzzahlige Lösungen zugelassen sind.
- Beispiel:
  Fermatsche Vermutung: $x^n + y^n = z^n$
  Für $n = 2$ heißen die diophantischen Lösungen ”pythagoräische Zahlentripel”.

Diophantische Gleichungen

- Lösungsverfahren (Gleichungssystem)
  -

$$
\begin{aligned}
cx_0 + c_1x_1 + \cdots + c_kx_k &= d && (7)\\
e_0x_0 + e_1x_1 + \cdots + e_kx_k &= f && (8)\\
\vdots \qquad\qquad\quad &\vdots && (9)\\
y_0x_0 + y_1x_1 + \cdots + y_kx_k &= z && (10)
\end{aligned}
$$

  - Finde von Null verschiedenen Koeffizienten c mit kleinstem Absolutwert im Gleichungssystem

Diophantische Gleichungen

- Lösungsverfahren (Fortsetzung)
  - Wenn $c = 1$, verwende die Gleichung, um die zu c gehörige Variable (hier o.B.d.A x_0) zu eliminieren
  - Wenn $c > 1$, prüfe, ob wenn $c_0 \bmod \mathrm{c} = \mathrm{c}_1 \bmod \mathrm{c} = \cdots = \mathrm{c}_\mathrm{k} \bmod \mathrm{c} = 0$, auch $d = 0$, ansonsten hat die Gleichung keine ganzzahligen Lösungen. Dividiere Gleichung durch c und eliminiere x_i wie oben.
  - Ist $c > 1$ und nicht alle $c_i \bmod \mathrm{c} = 0$, führe neue Variable ein:

$$\lfloor c/c \rfloor x_0 + \lfloor c_1/c \rfloor x_1 + \cdots + \lfloor c_k/c \rfloor x_k = t$$

  - Benutze t, um x_0 zu eliminieren:

$$ct + (c \bmod \mathrm{c}_1)\mathrm{x}_1 + \cdots + (\mathrm{c} \bmod \mathrm{c}_\mathrm{k})\mathrm{x}_\mathrm{k} = \mathrm{d}$$

Diophantische Gleichungen

- Beispiel:
  - $$\begin{aligned} 10w + 3x + 3y + 8z &= 1 \quad (11) \\ 6w - 7x - 5z &= 2 \quad (12) \end{aligned}$$
  - t_1 einführen:

    $$t_1 = 10/3w + 3/3x + 3/3y + 8/3z = 3w + x + y + 2z$$
  - y eliminieren:

    $$(10 \bmod 3)\mathrm{w} + (3 \bmod 3)\mathrm{x} + 3\mathrm{t}_1 + (3 \bmod 3)\mathrm{z} = \mathrm{w} + 3\mathrm{t}_1 + 2\mathrm{z} = 1$$

Diophantische Gleichungen

- Beispiel: (Fortsetzung)
  - w eliminieren:

$$6(1 - 3t_1 - 2z) - 7x - 5z = 2$$

$$7x + 18t_1 + 17z = 4$$

  - Wie vorhin neue Variable einführen:

$$x + 2t_1 + 2z = t_2$$

  - x eliminieren:

$$7t_2 + 4t_1 + 3z = 4$$

Diophantische Gleichungen

- Beispiel: (Fortsetzung)
  - Neue Variable einführen und z eliminieren:

$$2t_2 + t_1 + z = t_3$$

$$t_2 + t_1 + 3t_3 = 4$$

  - Nach t_2 auflösen und Einsetzen liefert schließlich die Lösung:

$$\begin{aligned} w &= 17 - 5t_1 - 14t_3 && (13)\\ x &= 20 - 5t_1 - 17t_3 && (14)\\ y &= -55 + 19t_1 + 45t_3 && (15)\\ z &= -8 + t_1 + 7t_3 && (16) \end{aligned}$$

Gauß Algorithmus

Gauß Algorithmus

- Lösen von linearen Gleichungssystemen
- Bereits bekannt aus der Mathematik

Gauß Algorithmus

- Lineares Gleichungssystem:

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1m}x_m &= b_1 && (17)\\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2m}x_m &= b_2 && (18)\\ \vdots &= \vdots && (19)\\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nm}x_m &= b_n && (20) \end{aligned}$$

  Matrixschreibweise:

$$A\vec{x} = \vec{b}$$

  Hier: nur $n \times n$ Matrizen.

- Eine Lösung: $\vec{x} = A^{-1}\vec{b}$
  Bestimmung von A^{-1} aufwendig. Lohnt sich nur, wenn man ein LGS für mehrere $\vec{b}$ lösen muss.

Gauß Algorithmus

- Operationen des Gauß Algorithmus:
  - Multiplizieren einer Zeile mit einem Faktor
  - Zeile i auf Zeile j addieren
  - Vertauschen von Zeilen

  Diese Operationen verändern die Lösungsmenge nicht.

Gauß Algorithmus

- Ziel:
  rechte obere Dreiecksmatrix:

$$
\begin{aligned}
a_{11}x_1 + a_{12}x_2 + a'_{13}x_3 + \cdots + a_{1n}x_n &= b_1 && (21)\\
a'_{22}x_2 + a'_{23}x_3 + \cdots + a'2nx_n &= b'_2 && (22)\\
\vdots &= \vdots && (23)\\
a'_{n-1,n-1}x_{n-1} + a'_{n-1,n}x_n &= b'_{n-1} && (24)\\
a'_{nn}x_n &= b'_n && (25)
\end{aligned}
$$

Gauß Algorithmus

- In dieser Form läßt sich die Lösung leicht finden:

$$x_n = \frac{b'_n}{a'_{nn}} \tag{26}$$

$$x_{n-1} = \frac{-a'_{n-1,n}x_n + b'_{n-1}}{a'_{n-1,n-1}} \tag{27}$$

- Allgemein:

$$x_i = \frac{1}{a_{ii}}\left(b_i - \sum_{k=i+1}^{n} a_{ik}x_k\right)$$

Gauß Algorithmus

- Wie kommt man nun zu so einer Dreiecksmatrix?
- Voraussetzung: Alle Diagonalelemente $a_{ii} \neq 0$ für alle $i = 1 \ldots n$ (Läßt sich durch Vertauschen von Zeilen herstellen).
- Spaltenweise ”nullen”.

  for $i \leftarrow 1$ to n:

    for $j \leftarrow i + 1$ to $n - 1$:

      Zeile j := Zeile j - Zeile $i \cdot \frac{a_{ji}}{a_{ii}}$

Gauß Algorithmus

- Algorithmus (Spalte $n+1$ ist $\vec{b}$):

  for $i \leftarrow 1$ to n:

    $dg \leftarrow a_{ii}$

    for $j \leftarrow i+1$ to n:

      $f_k \leftarrow \frac{a_{ji}}{dg}$

      for $k \leftarrow i$ to $n+1$:

        $a_{jk} = a_{jk} - f_k \cdot a_{ik}$

  for $i \leftarrow 1$ to n:

    $z_i \leftarrow a_{i,n+1}$

  for $i \leftarrow n$ downto 2:

    $dg \leftarrow a_{ii}$

    for $j \leftarrow i-1$ downto 1:

      $z_j \leftarrow z_j - z_i \cdot \frac{x_{ji}}{dg}$

  for $i \leftarrow 1$ to n:

    $z_i = \frac{z_i}{a_{ii}}$

Gauß Algorithmus

- Beispiel

$$x_1 + x_2 + x_3 = 0 \quad (28)$$
$$x_1 - x_2 + 2x_3 = 2 \quad (29)$$
$$4x_1 + x_2 - x_3 = 4 \quad (30)$$

- Erste Spalte eliminieren:

$$x_1 + x_2 + x_3 = 0 \quad (31)$$
$$-2x_2 + x_3 = 2 \quad (32)$$
$$-3x_2 - 5x_3 = 4 \quad (33)$$

Gauß Algorithmus

- Zweite Spalte eliminieren:

$$x_1 + x_2 + x_3 = 0 \quad (34)$$
$$-2x_2 + x_3 = 2 \quad (35)$$
$$-8.5x_3 = 1 \quad (36)$$

- Lösung:

$$\vec{x} = \begin{pmatrix} 1.2308 \\ -1.0769 \\ -0.1538 \end{pmatrix}$$

Gauß Algorithmus

- Alternative:
  Nach Division jeder Zeile i durch a_{ii}, erhält man eine Matrix der Form

$$\left(\begin{array}{ccccc|c} 1 & r_{12} & r_{13} & \cdots & r_{1n} & b_1 \\ l_{21} & 1 & r_{23} & \cdots & r_{2n} & b_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ l_{n1} & l_{n2} & l_{n3} & \cdots & 1 & b_n \end{array}\right)$$

Gauß Algorithmus

- Dieses LGS kann man aufsplitten in:

$$L = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ l_{21} & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ l_{n1} & l_{n2} & l_{n3} & \cdots & 1 \end{pmatrix} \tag{37}$$

$$R = \begin{pmatrix} 1 & r_{12} & r_{13} & \cdots & r1n \\ 0 & 1 & r_{23} & \cdots & r_{2n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix} \tag{38}$$

$$A = LR \tag{39}$$

Gauß Algorithmus

- (Fortsetzung)

$$A = LR \tag{40}$$

$$A\vec{x} = \vec{b} \tag{41}$$

$$L\vec{c} = \vec{b} \tag{42}$$

$$R\vec{x} = \vec{c} \tag{43}$$

- Ausblick: Pivotisierung

Literatur

- A.K. Dewdney - The new Turing omnibus
- Donald E. Knuth - Arithmetik (aus der Reihe TAOCP)
- Hans Grabmüller - Numerik 1 (für Ingenieure)
- Volker Strehl - Folien zur Einführung in die Theoretische Informatik 3
- Skiena, Revilla - Programming Challenges