Programmieren mit MuPAD - modulares Rechnen II

Thomas Wassong

Arbeitsgruppe Didaktik
FB 17 Mathematik
Universität Kassel
wassong@mathematik.uni-kassel.de

17. Dezember 2008

Der Chinesiche Restsatz

Der Chinesische Restsatz antwortet auf folgendes Problem:
Gegeben seien eine Reihe von Eigenschaften einer Zahl x in der Form:

$$\begin{aligned} x &\equiv l_1 \mod m_1 \\ x &\equiv l_2 \mod m_2 \\ &\vdots \\ x &\equiv l_n \mod m_n \end{aligned}$$

Der Chinesische Restsatz sagt nun, dass es dafür dann eine Lösung gibt, wenn die m_i jeweils paarweise teilerfremd sind. Der Beweis dieses Satzes gibt auch eine Algorithmus vor, mit dem sich dieses x berechnen lässt.

Algorithmus

```
Algorithmus chinesischer Restsatz:
Eingabe: zwei Listen [l_1,l_2,...,l_n]
und [m_1,m_2,...,m_n]
Ausgabe: Ein x, welches die Bedingungen erfüllt
1: berechne M=m_1 * m_2 * ... * m_n und p_i=M/m_i
2: berechne die Bezout-Koeffizienten r_i und s_i
zu p_i und m_i
3: xd=l_1 r_1 p_1 + l_2 r_2 p_2 + ... + l_n r_n p_n
4: return xd mod M
7: end if
```


Beispiel - Aufgabe

Ein Kartenspiel aus 56 numerierten Karten wird in 7 Zeilen und somit 8 Spalten ausgelegt. Dann wird ein Zuschauer gebeten sich eine Karte zu merken. Anschließend wird er gefragt, in welcher Spalte seine Karte liegt. Nun werden die Karten in der Reihenfolge eingesammelt, in der sie sich zu Anfang des Spieles befunden haben und anschließend in 8 Zeilen, also 7 Spalten ausgelegt. Der Zuschauer wird wieder gefragt, in welcher Spalte sich seine Karte befindet.
Die Frage lautet nun, welche Karte sich der Zuschauer gedacht hat.
Wir nehmen an, dass im ersten Fall die Karte in Spalte 4 gelegen hat und im zweiten Fall in Spalte 2.

Beispiel - Lösung

Nach dem Chinesischen Restsatz ergibt sich nun folgende Rechnung:
Berechnung von M und p_i: $M = 8 * 7 = 56$, $p_1 = \frac{56}{8} = 7$ und $p_2 = \frac{56}{7} = 8$.
Berechnung der Bézout-Koeffizienten:

$$1 = r_1 7 + s_1 8 \Rightarrow r_1 = -1 \text{ und } s_1 = 1$$

$$1 = r_2 8 + s_2 7 \Rightarrow r_2 = 1 \text{ und } s_2 = -1$$

Berechnung von xd:

$$xd = l_1 r_1 p_1 + l_2 r_2 p_2 = 4 * -1 * 7 + 2 * 8 * 1 = -12$$

Berechnung von x:

$$x = -12 \mod 56 = 44$$

Aufgabe

- Programmieren Sie den Algorithmus zum Chinesischen Restsatz unter Verwendung des EEA.
- Berechnen Sie eine Lösung zu folgendem Problem:

$$\begin{aligned} x &\equiv 2 \mod 3 \\ x &\equiv 3 \mod 4 \\ x &\equiv 1 \mod 7 \end{aligned}$$

der kleine Satz von Fermat

Der kleine Satz von Fermat hat folgende Aussage:

Für jedes $n \in \mathbb{N}$ und jede Primzahl $p \in \mathbb{P}$ gilt folgende Gleichung

$$n^p \equiv n \mod p.$$

Wir probieren diese Gleichung in MuPAD aus.

Beweis I

Wir beweisen den Satz von Fermat mit einer **vollständigen Induktion**. Das heißt, wir beweisen die Aussagen zunächst für $n = 1$. Danach setzten wir voraus, dass die Aussage für $n = k$ bewiesen ist, und versuchen mit diesem Wissen, die Aussage für $n = k + 1$ zu beweisen.
Im Endeffekt können wir damit sagen, dass wir die Aussage für alle möglichen n bewiesen haben, da jedes n Nachfolger von 1 ist.

Beweis II

Also beginnen wir mit dem Beweis für $n = 1$. Eingesetzt in die Gleichung ergibt sich folgende:

$$1^p \equiv 1 \mod p.$$

Diese Aussage ist natürlich für jede Primzahl p richtig.

Betrachten wir nun die Aussage für $n = k + 1$, wobei die Aussage für $n = k$ schon bewiesen ist.
Wir versuchen also folgende Gleichung zu beweisen:

$$(k+1)^p \equiv k + 1 \mod p.$$

Beweis III

$(k+1)^p$ können wir ähnlich der ersten binomischen Formel ausmultiplizieren. Es gilt dafür folgende Gleichung:

$$(k+1)^p = k^p + \binom{p}{1}k^{p-1} + \cdots + \binom{p}{p-1}k^1 + 1$$

mit

$$\binom{p}{r} = \frac{p(p-1)(p-2)\cdots(p-r+1)}{r(r-1)(r-2)\cdots 1} = p\frac{(p-1)!}{r!(p-r)!}.$$

Somit gilt

$$\binom{p}{r} \mod p = 0.$$

Beweis IV

Damit können wir nun folgende Gleichungskette aufbauen:

$$\begin{aligned}(k+1)^p &= \left(k^p + \binom{p}{1}k^{p-1} + \cdots + \binom{p}{p-1}k^1 + 1\right) \\ &= (k^p + 1) + \left(\binom{p}{1}k^{p-1} + \cdots + \binom{p}{p-1}k^1\right)\end{aligned}$$

Damit gilt:

$$\begin{aligned}(k+1)^p &\equiv (k^p + 1 + 0) \mod p \\ (k+1)^p &\equiv (k^p + 1) \mod p \\ (k+1)^p &\equiv (k+1) \mod p\end{aligned}$$

Nun ist die Aussage für $n = k + 1$ bewiesen und damit, im Rahmen der vollständigen Induktion, der kleine Satz von Fermat.

Die international standard book number

Um die Lagerverwaltung von Buchhändlern zu vereinfachen, wurde vor über 30 Jahren die **ISBN** eingeführt. Mit dieser, für jedes Buch eindeutigen Nummer, gestaltet sich die Übersicht der vorhandenen/verkauften Bücher und die Nachbestellung leichter
Die ISBN besitzt immer 10 Ziffern und hat folgenden Aufbau:

- der erste Ziffernblock steht für die Sprache, in der das Buch geschrieben wurde
- der zweite Ziffernblock repräsentiert den Verlag
- während der dritte Ziffernblock die verlagsinterne Buchnummer symbolisiert
- Die letzte Ziffer ist die Prüfziffer.

Die Prüfziffer bei einer ISBN

Die Prüfziffer ist notwendig, um Eingabe- oder Einlesefehler zu bemerken. Sie berechnet sich aus den vorherigen Ziffern der ISBN.
Um die Prüfziffer einer ISBN zu berechnen, werden die ersten 9 Ziffern aufsteigend mit $1, \ldots, 9$ multipliziert, aufaddiert und dann modulo 11 gerechnet. Das Ergebnis ist dann die Prüfziffer (für 10 wird ein X geschrieben)

Beispiel: zu der ISBN $3 - 86541 - 114 - 2$ gehört die Prüfziffer:

$$(3\cdot 1 + 8\cdot 2 + 6\cdot 3 + 5\cdot 4 + 4\cdot 5 + 1\cdot 6 + 1\cdot 7 + 1\cdot 8 + 4\cdot 9) \mod 11 = 2$$

Aufgabe

Schreiben Sie eine Prozedur, mit der Sie die Prüfziffer einer ISBN berechnen können.
Überprüfen Sie damit, ob folgende ISBNs richtig sein können:
$3 - 932975 - 00 - 6$
$3 - 507 - 73221 - 1$

European article number

Wie für die Buchändler, ist eine Lagerverwaltung auch für Supermärkte u.ä. wichtig. Auch hier gibt es eine Ziffernfolge, die **EAN**.
Die EAN besitzt immer 13 Ziffern und hat folgenden Aufbau:

- der erste Ziffernblock (2–3) steht für das Herstellungsland
- der zweite Ziffernblock repräsentiert die Herstellerfirma
- während der dritte Ziffernblock die firmainterne Produktnummer symbolisert
- Die letzte Ziffer ist wieder eine Prüfziffer.

Die Prüfziffer bei einer EAN

Die Prüfziffer ist notwendig, um Eingabe- oder Einlesefehler zu bemerken. Sie berechnet sich aus den vorherigen Ziffern der EAN.
Um die Prüfziffer einer EAN zu berechnen, werden die ersten 12 Ziffern abwechselnd mit 1 und 3 multipliziert, aufaddiert und dann das Negative der berechneten Zahl modulo 10 gerechnet. Das Ergebnis ist dann die Prüfziffer.

Beispiel: zu der EAN $978 - 3540 - 45377 - 2$ gehört die Prüfziffer:

$$-(9\cdot 1 + 7\cdot 3 + 8\cdot 1 + 3\cdot 3 + 5\cdot 1 + 4\cdot 3 + 0\cdot 1 + 4\cdot 3 + 5\cdot 1$$

$$+3\cdot 3 + 7\cdot 1 + 7\cdot 3) \mod 10 = 2$$

Aufgabe

Schreiben Sie eine Prozedur, mit der Sie die Prüfziffer einer EAN-Nummer berechnen können.
Überprüfen Sie damit, ob folgende EANs richtig sein können:
9 – 783540 – 453772
4 – 102560 – 081522

Ende

Frohe Weihnachten!