

Programmieren mit MuPAD - modulares Rechnen

Thomas Wassong

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

03. Dezember 2008

Übersicht

- 1 Fibonacci-Zahlen - reloaded
- 2 Der Euklidische Algorithmus
- 3 Der erweiterte euklidische Algorithmus

Thomas Wassong Programmieren mit MuPAD - modulares Rechnen 03. Dezember 2008

Die Fibonacci-Zahlen

Wir haben schon des Öfteren die Fibonacci-Zahlen hier in der Vorlesung besprochen. Hier nochmal die Definition:

$$\begin{aligned}F_1 &:= 1, \\F_2 &:= 1, \\F_n &:= F_{n-1} + F_{n-2}.\end{aligned}$$

Thomas Wassong Programmieren mit MuPAD - modulares Rechnen 03. Dezember 2008

eine schnellere Methode

Man hat herausgefunden, dass folgende Bedingungen für die Fibonacci-Zahlen gelten:

$$\begin{aligned}F_{2n} &= F_n(F_n + 2F_{n-1}) \\F_{2n+1} &= F_{n+1}^2 + F_n^2\end{aligned}$$

Bei genauerer Betrachtung fällt folgendes auf: Die Rekursionstiefe für die Berechnung Fibonacci-Zahl verringert sich erheblich. Somit verringert sich auch die Zeit zur Berechnung einer Fibonacci-Zahl. Dies wollen wir nun überprüfen.

Thomas Wassong Programmieren mit MuPAD - modulares Rechnen 03. Dezember 2008

Aufgabe

Die obige Vermutung werden wir nun überprüfen. Dazu folgende Aufgabenstellung:

- Programmieren Sie eine rekursive Prozedur zur Berechnung der Fibonacci-Zahlen nach der obigen Methode.
- Vergleichen Sie die Rechenzeiten Ihrer Funktion mit der eingebauten Funktion `numlib::fibonacci` für $n=1.000.000$.

Thomas Wassong Programmieren mit MuPAD - modulares Rechnen 03. Dezember 2008

Der Euklidische Algorithmus

Sie haben in der Vorlesung von Prof. Dr. Seiler den Euklidischen Algorithmus kennengelernt. Zur Wiederholung sehen Sie hier den Algorithmus in seiner rekursiven Form:

```
Algorithmus EA:
Eingabe: zwei natürliche Zahlen x und y mit x <= y
Ausgabe: d=ggt(x,y)
1: if x|y then
2:   return x
3: else
4:   return EA(y mod x, x)
5: end if
```

Thomas Wassong Programmieren mit MuPAD - modulares Rechnen 03. Dezember 2008

Aufgabe

Nun wollen wir diesen Algorithmus `EA` einmal in MuPAD umsetzen. Wir setzen dabei aber nicht zwingend voraus, dass $x \leq y$ gilt. Dazu folgende Bemerkung:

$x|y$ setzt man am Besten mit der Abfrage $(x \bmod y = 0)$ um. Berechnen Sie danach das Ergebnis von $\text{ggt}(1234, 56789)$.

Thomas Wassong Programmieren mit MuPAD - modulares Rechnen 03. Dezember 2008

Der erweiterte euklidische Algorithmus

Nachdem wir nun den Euklidischen Algorithmus programmiert haben, stellt sich noch die Frage nach den Bézout-Koeffizienten, also ganze Zahlen r und s , so dass gilt:

$$\text{ggt}(x, y) = r * x + s * y$$

z.B. $\text{ggt}(35, 126) = -7 * 35 + 2 * 126 = 7$, mit den Bézout-Koeffizienten $r = -7$ und $s = +2$.

Thomas Wassong Programmieren mit MuPAD - modulares Rechnen 03. Dezember 2008

Algorithmus EEA:

Eingabe: zwei natürliche Zahlen x und y mit $x \leq y$

Ausgabe: Eine Liste mit den Einträgen $[d, r, s]$,
wobei $d = \text{ggT}(x, y)$ und r und s die beiden
Bezout-Koeffizienten sind

```
1: if x|y then
2:   return [x,1,0]
3: else
4:   [g,rAlt,sAlt] = EEA(y mod x, x)
5:   r = sAlt - rAlt(y div x); s = rAlt;
6:   return [g,r,s]
7: end if
```

Programmieren Sie den erweiterten Euklidischen Algorithmus.