TECHNISCHE UNIVERSITÄT DRESDEN

Fachrichtung Mathematik · **Institut für Algebra** · Modul Math Ma ANGALG WiSe 2016/17

Dr. Jens Zumbrägel 17. Okt. 2016

1. Übungsblatt zur Angewandten Algebra

Arithmetik und euklidischer Algorithmus

1. Es sei der Prozessor-Befehl SUB gegeben:

   input $a, b \in \{0, \dots, B-1\},\ \varepsilon \in \{0, 1\}$
   output $c \in \{0, \dots, B-1\},\ \varepsilon^* \in \{0, 1\}$ so dass $a - b - \varepsilon = -\varepsilon^* B + c$

   Gib nun einen Algorithmus „Subtraktion“ für beliebige Zahlen $\alpha, \beta \in \mathbb{N}$ an.

2. Formuliere einen Algorithmus „Division mit Rest“, der bitweise ($B = 2$) arbeitet.

   (Hinweis: Verwende eine Subroutine „kleiner gleich“.)

3. Sei R ein euklidischer Ring, $a, b, c \in R$ und $\mathrm{ggT}(a, b) = 1$. Zeige:

   i) $a \mid bc$ impliziert $a \mid c$,

   ii) $a \mid c \ \wedge\ b \mid c$ impliziert $ab \mid c$.

4. Betrachte folgendes Codefragment in Sage (http://www.sagemath.org):

```
def ggt(a, b):
   if a == b: return a
   if is_even(a) and is_even(b): return 2*ggt(a/2, b/2)
   if is_even(a): return ggt(a/2, b)
   if is_even(b): return ggt(a, b/2)
   if a > b: return ggt((a-b)/2, b)
   return ggt((b-a)/2, a)
```

   Füge einen Befehl zur Ausgabe von Zwischenergebnissen ein. Teste dann den Code für die folgenden Zahlenpaare: a) $34, 21$ b) $136, 51$ c) $481, 325$ d) $8771, 3206$.

5. Betrachte den rekursiven Algorithmus aus der vorigen Aufgabe.

   i) Zeige, dass der Algorithmus korrekt arbeitet, d. h. für alle Inputs $a, b \in \mathbb{N}$ ist der Output $\mathrm{ggT}(a, b)$.

   ii) Finde eine Obergrenze für die Rekursionstiefe und zeige, dass der Algorithmus $O(n^2)$ Wortoperationen für Inputs der Länge n benötigt.

6. Sei R ein euklidischer Ring mit Gradfunktion $d : R \to \mathbb{N} \cup \{-\infty\}$, so dass d surjektiv ist und zusätzlich $d(ab) = da + db$, sowie $d(a + b) \leq \max\{da, db\}$ mit Gleichheit falls $da \neq db$, für alle $a, b \in R$ gilt. Zeige, dass R ein Polynomring über einem Körper ist.

   (Vorgehen: Zeige, dass $da = -\infty$ gdw. $a = 0$; zeige, dass $F = \{a \in R \mid da \leq 0\}$ ein Unterkörper von R ist; sei $X \in R$ mit $d(X) = 1$, zeige dass jedes $\alpha \in R \setminus \{0\}$ eine eindeutige Darstellung $\alpha = \sum_{i=0}^{n} a_i X^i$ mit $n = d\alpha$ und $a_i \in F$, $a_n \neq 0$ hat.)