Technische Universität München
Institut für Informatik
Prof. Tobias Nipkow, Ph.D.
Dr. Stefan Berghofer

SoS 2005
Aufgabenblatt 1
19. 4. 2005

Vorlesung Perlen der Informatik II

Aufgabe 1 Pratts Primzahlzertifikate

Schreiben Sie eine Funktion zur Überprüfung von Pratts Primzahlzertifikaten in ML. Ein Zertifikat besteht aus einer Liste von Regelanwendungen (Beweisschritten), wobei Regeln durch den Datentyp

```
datatype rule = Ax of int * int | R1 of int * int | R2 of int;
```

definiert sind. Hierbei wird das Axiom

$(p,\ x,\ 1)$

durch

`Ax (`p`, `x`)`

dargestellt, die Regel

$R_1: \quad (p,\ x,\ a),\ q \vdash (p,\ x,\ q * a) \qquad$ wenn $x^{(p-1)/q} \not\equiv 1 \bmod p$

durch

`R1 (`i`, `j`)`

wobei i und j die Nummern der Beweisschritte sind, in denen $(p,\ x,\ a)$ bzw. q gezeigt wurde. Die Regel

$R_2: \quad (p,\ x,\ p-1) \vdash p \qquad$ wenn $x^{p-1} \equiv 1 \bmod p$

wird durch

`R2 `i

dargestellt, wobei i die Nummer des Beweisschritts ist, in dem $(p,\ x,\ p-1)$ gezeigt wurde. Die im Beweissystem abgeleiteten Formeln p bzw. $(p,\ x,\ a)$ werden durch den Datentyp

```
datatype formula = Prime of int | Cand of int * int * int
```

dargestellt. Im Erfolgsfall soll die Überprüfungsfunktion eine Liste von Formeln ausgeben, wobei das letzte Element der Liste von der Form

`Prime `p

ist.