Mathematisches Institut
der Universität München
Helmut Schwichtenberg
Monika Seisenberger

Wintersemester 2002/2003
Blatt 2

Übungen zum Ferienkurs über Nichtnumerisches Programmieren

Aufgabe 5. Man bringe die rekursive `sum`-Definition in iterative Form. Dazu fülle man die offenen Stellen in folgendem Muster aus.

```
(define (sum summand-fct next-fct a b)
  (define (iter arg result)
    (if ??
        ??
        (iter ??
              ??)))
  (iter ?? ??))
```

Aufgabe 6. (a) Man schreibe eine Prozedur `expon`, die zu zwei gegebenen natürlichen Zahlen b und e (Basis und Exponent) die Potenz b^e berechnet.

(b) Man schreibe eine Prozedur `expmod`, die zu gegebenen Zahlen b, e und n die Zahl $b^e \mod n$ berechnet.

Aufgabe 7. Angenommen, Sie haben sich die Primzahlen $p = 47$ und $q = 59$ gewählt und deren Produkt $N = 2773$ sowie die Zahl $e = 17$ als Public Key veröffentlicht (e ist relativ prim zu $(p-1)(q-1)$). Jemand möchte Ihnen die Nachricht M übermitteln; er oder sie berechnet unter Verwendung Ihres Public-Keys $C = M^e \mod N$ und schickt Ihnen die verschlüsselte Nachricht

$$C = 1369$$

Wie lautet die ursprüngliche Nachricht? (Hinweis: SPACE = 00, A = 01, B = 02, C = 03, ... ,Z = 26).
Anleitung:

(a) Bestimmen Sie zunächst ein d mit

$$d * e = 1 \mod (p-1)(q-1).$$

$((d, (p-1)(q-1))$ ist der Private Key.)

(b) Entschlüsseln Sie die Nachricht, indem Sie $C^d \mod N$ berechnen.

Für Fortgeschrittene: $p = 34966941397$, $q = 290297328029$, $e = 65537$ und

$$C = 7036202717484935460960.$$

Abgabetermin. Mittwoch, den 2. Oktober 2002, in der Übung oder (besser) per email an `seisenb@mathematik.uni-muenchen.de`