HUMBOLDT–UNIVERSITÄT ZU BERLIN
MATHEMATISCH-NATURWISSENSCHAFTLICHE FAKULTÄT II
INSTITUT FÜR MATHEMATIK
PROF. PHD. ANDREAS GRIEWANK, VERTRETUNG: DR. JÜRGEN GEISER
DR. HANS-DIETRICH NIEPAGE, DIPL.-MATH. HOLGER HEITSCH
DIPL.-MATH. LUTZ LEHMANN

Humboldt-Universität zu Berlin, Institut für Mathematik, Unter den Linden 6, D-10099 Berlin

Übungsaufgaben zur Vorlesung Mathematik für Informatiker I

Serie 5. (Abgabe: bis 30.11.06)

Aufgabe 1:

a) Entscheiden Sie mit Hilfe des erweiterten Euklidischen Algorithmus, ob die Gleichung **6 Punkte**

$$(x * m) \bmod n = 1, \quad \text{d.h.,} \quad [x]_n * [m]_n = [1]_n$$

für die Paare $(m, n) = (947345, 6601), (897916, 344285)$ und $(607, 79048)$ eine Lösung x hat. Geben Sie, wann immer dies der Fall ist, die entsprechende Inverse $[x]_n = [m]_n^{-1}$ an und verifizieren Sie die Erfüllung der Gleichung.

b) Schreiben Sie eine Funktion in der Programmiersprache C (Pascal, Matlab, Maple, ...) mit Schnittstellendefinition **5 Punkte**

```
int inverse(int b, int a, int v, int s)
```

(oder ähnlich), welche sich selbst rekursiv aufruft, bis $a = 0$ erreicht wird. Der Wert

```
c = inverse(b,a,0,1)
```

soll dabei die folgenden Bedingungen erfüllen:

$$\begin{cases} c = -1, & \text{falls } \mathrm{GGT}(a, b) > 1 \\ (c * a) \bmod b = 1, & \text{sonst} \end{cases}$$

Aufgabe 2:
Lösen Sie für $m = 2231,\ n = 6507,\ r = 224,\ s = 3409$ das Paar von Gleichungen

$$x \bmod m = r \quad \text{und} \quad x \bmod n = s$$

a) mit Hilfe der in Lemma A.97 angegebenen Formel und unter Nutzung des erweiterten Euklidischen Algorithmus zur Berechnung der Inversen von $[m \bmod n]_n$ in $\mathbb{Z}_n$. **4 Punkte**

b) mittels des „direkten Verfahrens", d.h. in der Form $x = (x_m * m + x_n * n) \bmod (n * m)$. **4 Punkte**

phone: 030/2093-5820 fax: 030/2093-5848
e-mail: griewank@math.hu-berlin.de llehmann@math.hu-berlin.de heitsch@math.hu-berlin.de niepage@math.hu-berlin.de