UNIVERSITÄT DES SAARLANDES
Fachbereich 14 – Informatik

Prof. J. Buchmann
Stefan Neis

25. Oktober 1995

2. Übung zu

# "Algebra für Informatiker"

1. Man zeige, daß für ganze Zahlen $a, b, a_1, \ldots, a_k \neq 0$ gilt:
   (a) Für alle Primzahlen $p$ gilt $e(p, ab) = e(p, a) + e(p, b)$.
   (b) $a$ teilt $b$ genau dann, wenn $e(p, a) \leq e(p, b)$ gilt für alle Primzahlen $p$.
   (c) Es gilt $a = \pm b$ genau dann, wenn $e(p, a) = e(p, b)$ ist für alle Primzahlen $p$.
   (d) $\gcd(a_1, \ldots, a_k) = \prod_{p \in \mathbb{P}} p^{\min\{e(p,a_i):1 \leq i \leq k\}}$.
2. Zeige:
   (a) $a \equiv b \bmod m$ genau dann, wenn $a$ und $b$ denselben Rest bei der Division durch $m$ lassen.
   (b) Aus $a \equiv a' \bmod m$ und $b \equiv b' \bmod m$ folgt $ab \equiv a'b' \bmod m$.
3. In der Vorlesung haben wir einen effizienten Test auf Teilbarkeit durch 11 für Zahlen in Dezimaldarstellung gesehen. Im Rechner sind Zahlen jedoch in Binärdarstellung gegeben. Gib analoge Algorithmen für Tests auf Teilbarkeit durch $2^i \pm 1$, $i \in \mathbb{N}$, für Zahlen in Binärdarstellung an.
   Vergleiche ihre Laufzeit mit der Laufzeit einer Division mit Rest.
4. Zeige, daß aus $ab \equiv ac \bmod m$ folgt, daß auch $b \equiv c \bmod \frac{m}{\mathrm{ggT}(a,m)}$ gilt.

Abgabe:

Donnerstag, 2. 11. 1995