**Algebra I** 2.6.2004
**SoSe 2004**
**Schmale**

# Aufgabenblatt 7

(25) Beweisen Sie Beobachtung 10.7.

(26) Zeigen Sie im Kontext von §11:

(a) $N \subseteq G(R) \Leftrightarrow$ die Einbettung von $R$ in $R_{(N)}$ ist surjektiv

(b) Wenn $R = \mathbb{Z}_d,\ d \in \mathbb{N}_{\geq 2}$, dann ist $R_{(N)} \cong R$ für alle zulässigen $N$.

(27) Sei $R = K[x, y],\ K$ ein Körper. Weisen Sie nach, dass $I = xR + yR$ kein Hauptideal ist, und geben Sie in $I$ enthaltene maximale Hauptideale an.

(28) Eine kleine Anwendung der Vielfachheitenfunktionen $v_p$:

Sei $\mathcal{P}$ ein Vertretersystem für die Primelemente im faktoriellen Ring. $R$. Benutzen Sie die Definition 10.6, um für $a, b, c, \in < \mathcal{P} >$ zu zeigen:

$abc \cdot ggT(a, b, c) = kgV(a, b, c) \cdot ggT(a, b) \cdot ggT(b, c) \cdot ggT(c, a)$
Anleitung: Betrachten Sie bei festem Primelement $p$ jeweils und zunächst den Fall $''v_p$ (a) $\leq v_p$ (b) $\leq v_p(c)''$.
Bemerkung: Wenn $c = 1$, ergibt sich eine bekanntere Formel.

(29) (Zusatzangebot für Tüftler(innen))

**Der Rad-Algorithmus:**

```
Eingabe: N ∈ ℕ_{>7}
{s := ⌊√N⌋; (d_0, ..., d_7) := (4, 2, 4, 2, 4, 6, 2, 6); p := 1; }
Für q ∈ {2, 3, 5} : {Wenn ϱ_q(N) = 0 : p := q; }
Wenn p = 1 : {q := 7; k := 0,
        Solange q ≤ s :
                Wenn ϱ_q(N) = 0 : {p := q; q := s + 1; }
                sonst {q := q + d_k; k := ϱ_8(k + 1); }}
Ausgabe: Wenn  p = 1 :  N ist prim.
         Wenn  p > 1 :  N ist nicht prim und p ist ein Primteiler.
```

Zeigen Sie: Der Algorithmus erkennt für ein $N \geq 8$ ob $N$ prim ist **und** liefert, wenn $N$ nicht prim ist, einen Primteiler $p$.