Institut für Informatik
der Universität München
Prof. Martin Hofmann
Jan Hoffmann

WS 2008/09

08. Januar 2009

Übungen zur Vorlesung Komplexitätstheorie

Blatt 11

Aufgabe P-23: Zeigen Sie $\mathsf{IP} \subseteq \mathsf{PSPACE}$.

Aufgabe P-24: Zeigen Sie, dass es ein Orakel A gibt, so dass $\mathsf{IP}^A \neq \mathsf{PSPACE}^A$.

Was bedeutet das für den Beweis von $\mathsf{IP} = \mathsf{PSPACE}$?

Aufgabe H-11: Das Problem Quadratischer Rest ist definiert wie folgt.

Gegeben:	Zwei teilerfremde, natürliche Zahlen n, m mit $n < m$ und m, n teilerfremd.
Frage:	Gibt es eine natürliche Zahl x mit $x^2 \equiv n \mod m$?

Begründen Sie, warum der folgendene Algorithmus zeigt, dass das Komplement von Quadratischer Rest in der Klasse IP liegt.

```
Eingabe: n,m mit n < m
wähle zufällig z_1, z_2 mit z_i < m und z_i, m teilerfremd
wähle zufällig b_1, b_2 mit b_i ∈ {1,2}
for i = 1,2 do
      if b_i = 1 then w_i := z_i^2 mod m
      else w_i := n z_i^2 mod m
übertrage w_1, w_2 an P
empfange c_1, c_2 von P
for i = 1,2 do
      if b_i ≠ c_i then REJECT
ACCEPT
```

Hinweis: Beachten Sie, dass $nz_i^2 \mod m$ ein quadratischer Rest ist, genau dann, wenn n ein quadratischer Rest ist.

Abgabe der Hausaufgaben: Legen Sie Ihre Lösungen bitte bis spätestens **Mittwoch, 14.01.2009, 14 Uhr** in den Übungskasten vor **Raum F2** in der Oettingenstr. 67. **Besprechung** am Mittwoch, 14.01.2009.