**TECHNISCHE UNIVERSITÄT BERLIN** WS08/09
**Fakultät II – Institut für Mathematik**
Dozent: Prof. Dr. F. Heß
Assistent: G. Möhlmann
Abgabe: 20.1.09
www.math.tu-berlin.de/~hess/krypto-ws2008

# 11. Übung Kryptographie

## 1. Aufgabe

Sei die Notation wie im Skript zum quadratischen Sieb. Sei $w$ ein Vektor aus dem $\mathbb{Z}^r$ bei dem jede Koordinate gerade ist. Dann liegt $w$ im Kern von $M$, wenn ich jede Koordinate $\mod 2$ betrachte. Können die zu $w$ gehörigen Quadrate dazu benutzt werden, einen nicht-trivialen Teiler von $n$ zu finden?

**(4 Punkte)**

## 2. Aufgabe

Geben Sie eine Möglichkeit an, die Faktorbasis $S = \{p \in \mathbb{P} | p \leq B\}$ mit der Laufzeit $O(B \log(B))$ zu berechnen und begründen Sie, wie diese Laufzeit zustande kommt.

**(6 Punkte)**

## 3. Aufgabe

Sei auch hier die Notation wie im Skript zum quadratischen Sieb. In dem Abschnitt zum Siebschritt wird behauptet, dass wenn $f$ keine Nullstellen $\mod p$ besitzt, dann gibt es auch kein $x$ mit $f(x) \equiv 0 \mod p$ und wenn $f$ nur eine Nullstelle $\mod p$ besitzt, dann gilt $p = 2$ oder $N \equiv 0 \mod p$. Beweisen Sie das.

**(4 Punkte)**

## 4. Aufgabe

Über die nächsten beiden Hausaufgaben verteilt soll das quadratische Sieb programmiert werden. Diese Woche könnte man den Siebschritt implementieren und nächste Woche den Rest. Oder auch irgendwie anders. Auf jeden Fall finden sich auf der Website eine Datei mit einer Methode, die man dafür verwenden könnte, oder auch nicht.

**(6 Punkte)**