TECHNISCHE UNIVERSITÄT BERLIN WS09/10
Fakultät II – Institut für Mathematik
Dozent: Tobias Finis
Assistent: Gerriet Möhlmann
www.math.tu-berlin.de/~kant/kryptows09

7. Übung Kryptographie

1. Aufgabe

Sei die Notation wie aus der Vorlesung 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?

(5 Punkte)

2. Aufgabe

(a) Zeigt, dass für alle $N \in \mathbb{N}$ gilt:

$$N! = \prod_{p \leq N} p^{\sum_{k=1}^{\infty} \lfloor N/p^k \rfloor},$$

wobei das Produkt über Primzahlen p gebildet wird.

(b) Benutzt die Ungleichung

$$N! > \left(\frac{N}{e}\right)^N$$

um zu beweisen, dass

$$\sum_{p \leq N} \frac{\ln p}{p-1} > \ln N - 1$$

gilt.

(c) Folgert daraus, dass es unendlich viele Primzahlen gibt.

(6 Punkte)

3. Aufgabe

Sei die Notation wieder wie aus der ausgezeichneten Vorlesung zum quadratischen Sieb. Zeigt, dass wenn f keine Nullstellen $\mod p$ besitzt, dann gibt es auch kein x mit $f(x) \equiv 0 \mod p$ und dass wenn f nur eine Nullstelle $\mod p$ besitzt, $p = 2$ oder $N \equiv 0 \mod p$ gilt.

(4 Punkte)

4. Aufgabe

Programmiert den Miller-Rabin Primzahltest und benutzt ihn um die kleinste Primzahl, bei der fünf mal die Ziffer drei auftaucht, zu finden. Begründet, warum ihr wirklich die kleinste habt. **(5 Punkte)**