RUHR
UNIVERSITÄT
BOCHUM

RUB

Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Enrico Thomae

Präsenzübungen zur Vorlesung

Quantenalgorithmen

WS 2011/2012

Blatt 6 / 9. Januar 2012

AUFGABE 1:
Zeigen Sie, dass für $m \not| y$ gilt

$$\sum_{k=0}^{m-1} (e^{2\pi i \frac{y}{m}})^k = 0.$$

AUFGABE 2:
Berechnen Sie die Periode von $f(a) = 7^a \bmod 10$ mit Hilfe des in der Vorlesung angegebenen Quanten-Algorithmus. Wählen Sie dabei $M = 2^n = 2^7$ (d.h. $n = 7$) und nehmen Sie an, daß Sie in der ersten Messung den Wert 7 erhalten haben. Geben Sie die im Zuge des Algorithmus auftretenden Zwischenzustände an und berechnen Sie die Wahrscheinlichkeit, in der zweiten Messung einen der Werte $y = 32i$, $i = 0, \ldots, 3$ zu erhalten. Wie groß ist die Wahrscheinlichkeit, daß für die aus zwei Durchläufen des Algorithmus erhaltenen Werte y_1 und y_2 gilt, daß

1.) $y_1 y_2 \neq 0$, und

2.) das kleinste gemeinsame Vielfache von M/y_1 und M/y_2 die Periode von f ist?

AUFGABE 3:
Sei $M \in \mathbb{Z}$ mit $M > 1$ und $q = e^{2\pi i/M}$. Zeigen Sie, dass die Vektoren

$$v_n = \frac{1}{\sqrt{M}} (q^{nk})_{k=0,\ldots,M-1}$$

eine Orthonormalbasis des $\mathbb{C}^M$ bilden. Hierbei sei $\mathbb{C}^M$ wie gewöhnlich mit dem Skalarprodukt

$$\langle x \,|\, y \rangle = \sum_{i=0}^{M-1} x_i^* y_i$$

ausgestattet. Folgern Sie daraus, dass die Matrix

$$U = \frac{1}{\sqrt{M}} (q^{nk})_{n,k=0,\ldots,M-1}$$

unitär ist.