Prof. Dr. A. Goerdt
A. Oertel

TU Chemnitz
Sommersemester 2020
20. April 2020

Einführung Quantencomputing

1. Übung

Aufgabe 1: Führen Sie den Euklidischen Algorithmus für die Zahlen 16 und 7 aus. Beobachten Sie, dass sich durch $\mathrm{ggT}(16, 7) = 1$ eine Darstellung von $1 = 16 \cdot x + 7 \cdot y$ ergibt. Berechnen Sie diese x und y.

Aufgabe 2: Zeigen Sie die folgende Aussagen mit Hilfe der gegebenen Hinweise.

(a) *Aussage:* Sei $\varphi(n) \coloneqq \left|\{i \in \mathbb{N} | 1 \leq i \leq n \wedge \mathrm{ggT}(i, n) = 1\}\right|$ die *Eulersche φ-Funktion.* Für a mit $1 \leq a \leq n-1$ und $\mathrm{ggT}(a, n) = 1$ gilt

$$a^{\varphi(n)} \equiv 1 \bmod n.$$

Hinweis: Benutzen Sie, dass die Menge $\mathbb{Z}_n^* = \{i \in \mathbb{N} | 1 \leq i \leq n \wedge \mathrm{ggT}(i, n) = 1\} = \{x_1, \ldots, x_{\varphi(n)}\}$ alle multiplikativ invertierbaren Zahlen modulo n enthält. Außerdem gilt für $y \in \mathbb{Z}_n^*$, dass $\{x_1, \ldots, x_{\varphi(n)}\} = \{y \cdot x_1, \ldots, y \cdot x_{\varphi(n)}\}$.

(b) *Aussage:* Der *Satz von Fermat* aus der Vorlesung. Für eine Primzahl n und a mit $1 \leq a \leq n-1$, $(\mathrm{ggT}(a, n) = 1)$ gilt

$$a^{n-1} \equiv 1 \bmod n.$$

Das ist äquivalent zu

$$a^n \equiv a \bmod n.$$

Hinweis: Zeigen Sie zunächst die Aussage für $a = 2 = 1 + 1$ mit Hilfe des *Binomischen Satzes*

$$(x + y)^n = \sum_{i=0}^{n} \binom{n}{i} \cdot x^{n-i} \cdot y^i = \sum_{i=0}^{n} \frac{n!}{i! \cdot (n-i)!} \cdot x^{n-i} \cdot y^i.$$

Was können Sie über den Binominialkoeffizienten modulo n sagen, wenn n eine Primzahl ist?

Zeigen Sie nun die Aussage für beliebiges $a = 1 + 1 + \ldots + 1$. Benutzen Sie das *Multinomialtheorem*

$$(x_1 + \ldots + x_k)^n = \sum_{i_1 + \ldots + i_k = n} \frac{n!}{i_1! \cdot \ldots \cdot i_k!} \cdot x_1^{i_1} \cdot \ldots \cdot x_k^{i_k}$$

und gehen analog wie für $a = 2$ vor.

Aufgabe 3: Stellen Sie die folgenden Zuweisungen in der Matrix-Schreibweise dar.

(a) $x \coloneqq 0$

(b) $x \coloneqq 1$

(c) $x \coloneqq y$

(d) $x \coloneqq \neg y$

(e) $y \coloneqq \text{if } x = 1 \text{ then } \neg y \text{ else } y$