Prof. Dr. A. Goerdt
A. Oertel

TU Chemnitz
Sommersemester 2020
18. Juni 2020

Einführung Quantencomputing

Lösungen zur 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.

Lösung 1:

$$\begin{array}{ccc} 16 = 7 \cdot 2 + 2 & & 2 = 16 - 7 \cdot 2 \rightarrow 1 = 7 - (16 - 7 \cdot 2) \cdot 3 = 7 \cdot 7 - 16 \cdot 3 + \\ \downarrow & & \uparrow \\ 7 = 2 \cdot 3 + 1 & & 1 = 7 - 2 \cdot 3 \\ \searrow & & \nearrow \end{array}$$

Daraus folgt

$x = -3$
$y = 7.$

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.

Lösung 2:

(a) Mit $y = a$ gilt

$$1 \equiv x_1 \cdot \ldots \cdot x_{\varphi(n)} \equiv a \cdot x_1 \cdot \ldots \cdot a \cdot x_{\varphi(n)} \equiv a^{\varphi(n)} \cdot x_1 \cdot \ldots \cdot x_{\varphi(n)} \equiv a^{\varphi(n)} \bmod n.$$

Daraus folgt

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

(b) Wir nutzen

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

Wir verwenden den *Binomischen Satz* für $(1+1)^n$.

$$(1+1)^n \equiv \sum_{i=0}^{n} \frac{n!}{i! \cdot (n-i)!} \cdot 1^{n-i} \cdot 1^i \equiv \sum_{i=0}^{n} \frac{n!}{i! \cdot (n-i)!} \bmod n$$

Der Binominialkoeffizient wird von n geteilt, wenn das n im Zähler nicht gekürzt wird. Es wird nur gekürzt, wenn n auch als Faktor im Nenner steht, da n eine Primzahl ist. Dies ist nur bei

$$i = 0,\ i = n$$

der Fall und für diese i ist der Binominialkoeffizient 1.

Somit gilt

$$(1+1)^n \equiv 1+1 \bmod n.$$

Benutzen wir nun das *Multinomialtheorem* für $a = \underbrace{1+\ldots+1}_{a \text{ Mal}}$.

$$(1+\ldots+1)^n \equiv \sum_{i_1+\ldots+i_a=n} \frac{n!}{i_1! \cdot \ldots \cdot i_a!} \cdot 1^{i_1} \cdot \ldots \cdot 1^{i_a} \equiv \sum_{i_1+\ldots+i_a=n} \frac{n!}{i_1! \cdot \ldots \cdot i_a!} \bmod n$$

Mit der gleichen Argumentation wie für den Binominialkoeffizienten, ist der Multinomialkoeffizient teilbar durch n, wenn im Nenner kein n als Faktor vorkommt. Dies ist nur der Fall, wenn für ein $j \in \{1, \ldots, a\}$

$$i_j = n \text{ und } i_\ell = 0 \text{ für } 1 \leq \ell \leq a, \ell \neq j$$

und der Rest der i muss 0 sein.

Dafür gibt es a Möglichkeiten und der Multinomialkoeffizient ist immer 1. Daraus ergibt sich

$$\begin{aligned}(1+\ldots+1)^n = (1+\ldots+1)^n &\equiv (1+\ldots+1) \bmod n \\ a^n &= a \bmod n\end{aligned}$$

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

Lösung 3:

(a)

$$0 \to 0$$
$$1 \to 0$$
$$\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$$

(b)

$$0 \to 1$$
$$1 \to 1$$
$$\begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$$

(c)

$$00 \to 00$$
$$01 \to 11$$
$$10 \to 00$$
$$11 \to 11$$

$$\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

(d)

$$00 \to 10$$
$$01 \to 01$$
$$10 \to 10$$
$$11 \to 01$$

$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

(e)

$$00 \to 00$$
$$01 \to 01$$
$$10 \to 11$$
$$11 \to 10$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$