2.3 Die Wahrscheinlichkeit der Faktorisierung

Sei $n \in \mathbb{N}_3$. Ferner sei zunächst $u \in \mathbb{N}_2$ beliebig gerade, $u = r \cdot 2^s$ mit ungeradem r und $s \geq 1$. Dazu werden folgende Mengen eingeführt:

$$\begin{aligned}
A_u^{(0)} &= B_u^{(0)} := \{w \in \mathbb{M}_n \mid w^r = 1\} \quad [\text{Fall } (\mathrm{E}_{n,u}/\mathrm{I})],\\
A_u^{(t)} &:= \{w \in \mathbb{M}_n \mid w^{r\cdot 2^t} = 1, w^{r\cdot 2^{t-1}} \neq 1\} \quad \text{für } 1 \leq t \leq s,\\
B_u^{(t)} &:= \{w \in A_u^{(t)} \mid w^{r\cdot 2^{t-1}} = -1\} \quad [\text{Fall } (\mathrm{E}_{n,u}/\mathrm{II})],\\
A_u &:= \bigcup_{t=0}^{s} A_u^{(t)} = \{w \in \mathbb{M}_n \mid w^u = 1\},\\
B_u &:= \bigcup_{t=0}^{s} B_u^{(t)} \quad [\text{Fall } (\mathrm{E}_{n,u}) \text{ (I oder II)}].\\
C_0 &:= \{w \in \mathbb{M}_n \mid \operatorname{Ord} w \text{ ungerade}\},\\
C_1 &:= \{w \in \mathbb{M}_n \mid -1 \in \langle w \rangle\},\\
C &:= C_0 \cup C_1.
\end{aligned}$$

Bemerkungen.

1. $A_u^0 \leq A_u \leq \mathbb{M}_n$ sind Untergruppen, ebenso $A_u^0 \leq C_0 \leq \mathbb{M}_n$.
2. $B_u^{(t)} = A_u^{(t)} \cap C$ für $t = 0, \ldots, s$, denn in einer zyklischen Gruppe $\langle w \rangle$ kann es außer 1 nur eine weitere Quadratwurzel aus 1 geben.
3. Also gilt auch $B_u = A_u \cap C$.
4. B_u ist im Fall von Abschnitt 2.2 genau die Ausnahmemenge mit $(\mathrm{E}_{n,u})$, die nicht zur Faktorisierung von n führt. Der folgende Satz sagt aus, dass die Wahrscheinlichkeit, zufällig ein Element dieser Ausnahmemenge zu erwischen, $< \frac{1}{2}$ ist; probiert man der Reihe nach k zufällige Elemente, ist die Wahrscheinlichkeit, n nicht faktorisiert zu haben, $< 1/2^k$, wird also sehr schnell *extrem* klein.

Satz 1 *Sei n ungerade und keine Primpotenz. Sei $u = r \cdot 2^s$ ein Vielfaches von $\lambda(n)$ mit ungeradem r. Dann ist*

$$\#B_u \leq \frac{1}{2} \cdot \varphi(n).$$

Beweis. Nach dem *folgenden Hilfssatz* ist C und damit erst recht B_u in einer echten Untergruppe von $\mathbb{M}_n$ enthalten. $\diamond$

Hilfssatz 1 (Dixon, AMM 1984) *Sei $n \in \mathbb{N}_3$. Ferner sei $\langle C \rangle = \mathbb{M}_n$. Dann ist n eine Primpotenz oder das Zweifache einer solchen.*

Beweis. Sei in diesem Beweis $\lambda(n) = r \cdot 2^s$ mit ungeradem r. (Da $n \geq 3$, ist $s \geq 1$.) Sei

$$h : \mathbb{M}_n \longrightarrow \mathbb{M}_n, \qquad w \mapsto w^{r \cdot 2^{s-1}}.$$

Dann ist h Gruppen-Homomorphismus mit $h(\mathbb{M}_n) \subseteq \{v \in \mathbb{M}_n \mid v^2 = 1\}$ (Gruppe der zweiten Einheitswurzeln $\bmod n$). Da die $w \in C_0$ ungerade Ordnung haben, ist $h(C_0) \subseteq \{1\}$. Für $w \in C_1$ ist $h(w) \in \langle w \rangle$ und $h(w)^2 = 1$, also w eine der beiden Einheitswurzeln $\pm 1 \in \langle w \rangle$.

Insgesamt ist $h(C) \subseteq \{\pm 1\}$.

Ist n keine Primpotenz, so $n = pq$ mit teilerfremden $p, q \in \mathbb{N}_2$. Da $2^s | \lambda(n) = \mathrm{kgV}(\lambda(p), \lambda(q))$, können wir o. B. d. A. $2^s | \lambda(p)$ annehmen. Nach dem chinesischen Restsatz gibt es ein $w \in \mathbb{M}_n$ mit $w \equiv 1 \pmod{q}$, so dass $w \bmod p$ die Ordnung 2^s hat. Dann ist $h(w) \not\equiv 1 \pmod{p}$, also erst recht $h(w) \neq 1$. Da $h(w) \equiv 1 \pmod{q}$, ist auch $h(w) \neq -1$ – außer wenn $q = 2$.

Also ist $h(\mathbb{M}_n) \not\subseteq \{\pm 1\}$, es sei denn, n erfüllt die Behauptung des Hilfssatzes. $\diamond$