Aufgabe 6

(a) Zeigen Sie, dass 85 eine Pseudoprimzahl zur Basis 4 ist.

(b) Ist 85 auch eine *starke* Pseudoprimzahl zur Basis 4?

Definition 3.4.1 Eine natürliche Zahl $n > 1$ heißt *Pseudoprimzahl zur Basis b*, falls n zusammengesetzt ist, $ggT(b, n) = 1$ und $b^{n-1} \equiv 1 \pmod{n}$ gilt.

Lemma 3.4.8 *Sei p eine ungerade Primzahl und schreibe*

$$p - 1 = 2^s t, \qquad \text{mit } t \text{ ungerade.}$$

Sei b eine natürliche Zahl, die nicht von p teilbar ist. Es gilt

(a) entweder $b^t \equiv 1 \pmod{p}$,

(b) oder $b^{2^i t} \equiv -1 \pmod{p}$ für ein i mit $0 \le i < s$.

Definition 3.4.9 (a) Eine ungerade, zusammengesetzte Zahl n heißt *starke Pseudoprimzahl* zur Basis b, falls n teilerfremd zu b ist und die Bedingung von Lemma 3.4.8 erfüllt ist.

a) $ggT(85,4) = 1$

$5 \cdot 17 \quad 2 \cdot 2$

$85 = 21 \cdot 4 + 1$

Nach Lemma von Bezout folgt $ggT(85,4) = 1$

$4^{85-1} = 4^{84}$

$4^2 = 16$

$4^3 = 16 \cdot 4 = 64$

$4^4 = 64 \cdot 4 = 256 \equiv 3 \cdot 85 + 1 \equiv 1 \bmod 85$

$256 : 85 = 3 \text{ R } 1$

$60 \cdot 4 + 4 \cdot 4$

$4^{84} \equiv (4^4)^{21} \equiv 1^{21} \equiv 1 \bmod 85$

Sei $z \in \mathbb{Z}$, $\overline{z} := z + 85\mathbb{Z} \in \mathbb{Z}/85\mathbb{Z}$

$\overline{4^{84}} = \overline{(4^4)^{21}} = \overline{4^4}^{21} = \overline{1}^{21} = \overline{1}$

$\overline{1} \equiv \overline{86} \rightarrow 1 \equiv 86 \bmod 85$

$\overline{4 \cdot 5} = \overline{4} \cdot \overline{5} \rightarrow$

$\Rightarrow$ Nach Def folgt Behauptung

$ggT(85,4) = 1$

$n - 1 = 85 - 1 = 84 = 2^2 \cdot 21$

$\Rightarrow s = 2, \; t = 21$ $\quad 2 \cdot 42 = 2 \cdot 2 \cdot 21 = 2 \cdot 2 \cdot 3 \cdot 7$

$4^{21} \pmod{85}$

$4^{21} \equiv 4^{20} \cdot 4 \equiv (4^4)^5 \cdot 4 \equiv 1 \cdot 4 \equiv 4 \not\equiv 1 \bmod 85$

$\Rightarrow$ a) nicht erfüllt (aus Lemma)

$b^{2^i t} = (b^{2^i})^t$

$i = 0$: $b^{2^0 t} \equiv b^{2^0 \cdot t} \equiv b^t \equiv 4 \not\equiv -1 \bmod 85$

$i = 1$: $b^{2^i \cdot t} \equiv 4^{2 \cdot 21} \equiv (4^{21})^2 \equiv 4^2 \equiv 16 \not\equiv -1 \pmod{85}$

$\equiv 4^{42} = 4^{40} \cdot 4^2 \equiv (4^4)^{10} \cdot 4^2$

$\equiv 1^{10} \cdot 16 \equiv 16 \pmod{85}$

$\Rightarrow$ b) von Lemma 3.4.8 ist nicht erfüllt

$\Rightarrow$ 85 ist keine starke Pseudoprim.