

Aufgabe 6

- (a) Zeigen Sie, dass 85 eine Pseudoprimalzahl zur Basis 4 ist.  
 (b) Ist 85 auch eine starke Pseudoprimalzahl zur Basis 4?

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

Lemma 3.4.8 Sei  $p$  eine ungerade Primzahl und schreibe

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

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  $0 \leq i < s$ .

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

a)  $\text{ggT}(85, 4) = 1$   
 $\begin{matrix} // & // \\ 5 \cdot 17 & 2 \cdot 2 \end{matrix}$

$$85 = 21 \cdot 4 + 1$$

Nach Lemma von Bezout folgt  $\text{ggT}(85, 4) = 1$

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

$$4^2 = 16$$

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

$$4^4 = 64 \cdot 4 = 256 = 3 \cdot 85 + 1 \equiv 1 \pmod{85}$$

$$\uparrow$$

$$60 \cdot 4 + 4 \cdot 4$$

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

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

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

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

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

$\Rightarrow$  Nach Def folgt Behauptung

$$\text{ggT}(85, 4) = 1$$

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

$$\Rightarrow s=2, t=21$$

$$\begin{matrix} 2 \cdot 42 \\ = 2 \cdot 2 \cdot 21 \\ = 2 \cdot 2 \cdot 3 \cdot 7 \end{matrix}$$

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

$$4^{21} = 4^{20} \cdot 4 \stackrel{\text{aus Lemma}}{=} (4^4)^5 \cdot 4 \equiv 1 \cdot 4 \equiv 4 \pmod{85}$$

$\Rightarrow$  a) nicht erfüllt

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

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

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

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

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

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

$\Rightarrow$  85 ist keine starke Pseudoprimalzahl.