Kryptologie

Übung, LVA 405.321
C. Fuchs

10. Übungsblatt, SS 2022

25.05.2022

1. Beweise die folgenden Aussage: Für jede Basis $a \in \mathbb{Z}$ existieren unendlich viele a-Pseudoprimzahlen. (Hinweis: Zeige, dass für jede ungerade Primzahl p die $a(a^2-1)$ nicht teilt, die Zahl $((a^p-1)/(a-1))((a^p+1)/(a+1))$ eine a-Pseudoprimzahl ist.)

2. Seien p und q Primzahlen, $n = pq$ und $d = \text{ggT}(p-1, q-1)$. Zeige, dass n genau dann eine Pseudoprimzahl zur Basis b ist, falls $b^d \equiv 1 \pmod{n}$.

3. Angenommen n ist ungerade, zusammengesetzt und keine Carmichael-Zahl. Zeige, dass höchstens die Hälfte der Zahlen a mit $\text{ggT}(a, n) = 1$ und $a \leq n$ die Gleichung $a^{n-1} \equiv 1 \pmod{n}$ erfüllen.

4. Bestimme eine Carmichael-Zahl, die das Produkt von 4 Primzahlen ist.