Übungen zur Vorlesung Kryptographie

Abt. Reine Mathematik SS 06 – Blatt 3

Abgabetermin: Fr., 19.05.2006 um 12:30 Uhr vor Beginn der Übung

---

1. Berechne die folgenden Ausdrücke, falls sie existieren:
   (a) $\overline{201}^{-1} \in \mathbb{Z}/291\mathbb{Z}$
   (b) $\overline{67}^{-1} \in \mathbb{Z}/97\mathbb{Z}$
   (c) $\overline{7}^{-1} \cdot \overline{42} \in \mathbb{Z}/499\mathbb{Z}$
2. Zeige: Für jedes $n \in \mathbb{N}$ gilt: $n^{13} \equiv n \pmod{210}$.
3. (a) Bestimme die letzten zwei Stellen von 2^{392}
   (b) Bestimme die letzten drei Stellen von $7^{(7^{100000})}$
4. (a) Finde die kleinste Primitivwurzel mod 17 .
   (b) Sei a diese Primitivwurzel. Finde ein $x \in \mathbb{N}$ mit $a^x \equiv 11 \pmod{17}$
5. Die Eulersche ϕ-Funktion:
   (a) Für welche $n \in \mathbb{N}$ gilt $\phi(2n) = \phi(n)$?
   (b) Gibt es ein $n \in \mathbb{N}$ mit $\phi(n) = 14$?