

Diskrete Logarithmierung

Aufgabe 1. Berechnen Sie $3^{123} \pmod{100}$.

Aufgabe 2. Seien q eine Primzahl und a ein Element aus der multiplikativen Gruppe $\mathbb{Z}_q^* = \{1, 2, \dots, q-1\}$. Beweisen Sie, daß a genau dann die Gruppe \mathbb{Z}_q^* erzeugt, wenn für alle Primteiler p der Zahl $q-1$ gilt

$$a^{(q-1)/p} \not\equiv 1 \pmod{q}.$$

Aufgabe 3. Bestimmen Sie, daß 5 ein Erzeugendes der Gruppe \mathbb{Z}_{43}^* ist.

Aufgabe 4. Finden Sie alle Lösungen der Kongruenz mit Hilfe des Pohlig-Hellman Algorithmus.

$$3 \equiv 5^x \pmod{43}.$$

Aufgabe 5. Finden Sie alle Lösungen der Kongruenz mit Hilfe des Babystep-Giantstep Algorithmus.

$$2 \equiv 3^x \pmod{101}.$$

Aufgabe 6. Finden Sie alle Lösungen der Kongruenz mit Hilfe des Pollard- ρ Algorithmus.

$$2 \equiv 3^x \pmod{17}.$$