Übungsblatt 1

Kryptographie und Kodierungstheorie
WiSe 16/17

Aufgabe 1.1. (Teiler und Primzahlen)

(a) Bestimmen Sie die Anzahl der Teiler von 2^n, $n \in \mathbb{Z}_{\geq 0}$.

(b) Bestimmen Sie alle Teiler von 195.

(c) Berechnen Sie die Primfaktorzerlegung von 37800.

(d) Zeigen Sie, dass jede zusammengesetzte Zahl $n > 1$ einen Primteiler $p \leq \sqrt{n}$ hat.

Aufgabe 1.2. (Euklidischer Algorithmus)

(a) Berechnen Sie gcd(235,124) samt seiner Darstellung mit dem erweiterten Euklidischen Algorithmus.

(b) Finden Sie eine Folge $(a_i)_{i\geq 1}$ positiver ganzer Zahlen mit der Eigenschaft, dass der Euklidische Algorithmus genau i Iterationen benötigt, um $\gcd(a_{i+1}, a_i)$ zu berechnen.

Aufgabe 1.3. (Invertierung modulo m)

(a) Lösen Sie $122x \equiv 1 \bmod 343$.

(b) Bestimmen Sie alle invertierbaren Restklassen modulo 25 und berechnen Sie alle Inverse.

Aufgabe 1.4. (Ordnungen)

(a) Berechnen Sie die Ordnung von 2 mod 1237.

(b) Bestimmen Sie die Ordnung aller Elemente in $(\mathbb{Z}/15\mathbb{Z})^*$.

Aufgabe 1.5. (Primitivwurzeln und quadratische Reste)

(a) Bestimmen Sie für $g = 2, 3, 5, 7, 11$ jeweils eine Primzahl $p > g$ mit der Eigenschaft, dass g eine Primitivwurzel mod p ist.

(b) Sei p eine Primzahl, $p \equiv 3 \bmod 4$. Sei a eine ganze Zahl, die ein Quadrat mod p ist (d.h. die Kongruenz $a \equiv b^2 \bmod p$ hat eine Lösung). Zeigen Sie, dass $a^{\frac{p+1}{4}}$ eine Quadratwurzel von a mod p ist.