9. Übung Kryptographie

1. Aufgabe

- (a) Ein $n \in \mathbb{N}$ heißt zusammengesetzt, falls n nicht prim ist. Sei n eine zusammengesetzte ungerade Zahl für die

$$a^{n-1} \equiv 1 \pmod{n}$$

gilt für ein $a \in \mathbb{Z}$. Solch eine Zahl nennt man Pseudoprimzahl zur Basis a . Ist n für alle $a \in \mathbb{Z}$ mit $\gcd(a, n) = 1$ eine Pseudoprimzahl zur Basis a , so nennt man n Carmichael-Zahl. Man nennt $n \in \mathbb{N}$ quadratfrei, wenn es kein $p \in \mathbb{P}$ gibt mit $p^2 | n$. Zeigen Sie, dass eine Carmichael-Zahl mindestens drei verschiedene Primteiler hat.

Benutzen Sie dazu die folgende Aussage aus der Übung:

$$n \text{ ist Carmichael-Zahl} \Leftrightarrow n \text{ ist quadratfrei und es gilt: } p|n \Rightarrow (p-1)|(n-1) \quad (p \in \mathbb{P}).$$

- (b) Zeigen Sie, dass $N = 294409$ eine Carmichael-Zahl ist.
- (c) Zeigen Sie, dass $M = (6k+1)(12k+1)(18k+1)$ eine Carmichael-Zahl ist, falls $6k+1, 12k+1, 18k+1 \in \mathbb{P}$ für $k \in \mathbb{N}$ sind.

(6 Punkte)

2. Aufgabe

Sei n eine zufällige natürliche Zahl einer gewissen Größenordnung. Das heißt es gibt eine Schranke N mit $N \leq n \leq 2N$. Der Solovay-Strassen Zusammengesetztheitstest findet für n mit Wahrscheinlichkeit größer $1/2$ raus, dass sie zusammengesetzt ist, wenn n wirklich zusammengesetzt ist. Berechne die Wahrscheinlichkeit dafür, dass n prim ist, wenn der Algorithmus k mal sagt: „ n ist nicht zusammengesetzt“.

Diese Aufgabe ist fummeliger als sie scheint. Man muss sich mit bedingten Wahrscheinlichkeiten und Primzahlverteilungen rumschlagen.

(5 Punkte)

3. Aufgabe

Sei p eine ungerade Primzahl und $a \in \mathbb{Z}$. Dann gilt:

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}.$$

(4 Punkte)

4. Aufgabe

Implementieren sie den Solovay-Strassen Primzahltest aus der Übung. Schreiben Sie sich dazu eine Funktion, die den Wert des Jacobi Symbols mittels der in der Vorlesung angegebenen Rechenregeln ermittelt. Berechnen Sie die größte Primzahl unter 10^{10} mit ihrem Algorithmus.

(5 Punkte)