TECHNISCHE UNIVERSITÄT BERLIN WS09/10
Fakultät II – Institut für Mathematik
Dozent: Tobias Finis
Assistent: Gerriet Möhlmann
www.math.tu-berlin.de/~kant/kryptows09

4. Übung Kryptographie

1. Aufgabe

Berechnet die folgenden Ausdrücke unter Verwendung der Regeln für das Jacobi Symbol:

(a) $\left(\frac{4628}{6409}\right)$

(b) $\left(\frac{8085}{8731}\right)$

(4 Punkte)

2. Aufgabe

Seien p eine ungerade Primzahl mit $p \equiv 5 \mod 8$ und a ein quadratischer Rest modulo p. Zeigt, dass entweder $\pm a^{(p+3)/8}$ modulo p oder $\pm 2a(4a)^{(p-5)/8}$ modulo p quadratische Wurzeln von a modulo p sind.

(6 Punkte)

3. 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. Berechnt 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.

(4 Punkte)

4. Aufgabe

Implementiert den Solovay-Strassen Primzahltest aus der Übung. Schreibt euch dazu eine Funktion, die den Wert des Jacobi Symbols mittels der in der Übung angegebenen Rechenregeln ermittelt. Berechnt die größte Primzahl unter 10^{10} mit eurem Algorithmus.

(6 Punkte)