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

5. Übung Kryptographie

1. Aufgabe

Zeigt, dass die folgenden Zahlen in C_3 (siehe Vorlesung) enthalten sind.

(a) Zahlen der Form $(m+1)(2m+1)$ mit $m+1, 2m+1 \in \mathbb{P}$ und ungerade.

(b) Zahlen der Form $(m+1)(3m+1)$ mit $m+1, 2m+1 \in \mathbb{P}$ und beide kongruent $3 \mod 4$.

(c) 25.

(5 Punkte)

2. Aufgabe

(a) Sei n eine zusammengesetzte ungerade Zahl für die

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

gilt für ein $a \in \mathbb{Z}$. Solch eine Zahl nennt man (Fermat-)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 $p^2|n$. Zeigt, dass eine Carmichael-Zahl mindestens drei verschiedene Primteiler besitzt.

Benutzt dazu die folgende Aussage:

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

(b) Zeigt, dass $N = 294409$ eine Carmichael-Zahl ist.

(c) Zeigt, dass $M = (6k+1)(12k+1)(18k+1)$ eine Carmichael-Zahl ist, falls $6k+1, 12k+1, 18k+1 \in \mathcal{P}$ für $k \in \mathbb{N}$ sind. Folgt daraus schon, dass es unendlich viele Carmichael-Zahlen gibt?

(5 Punkte)

3. Aufgabe

Ein Geheimnis ist mit Shamir's Secret Sharing auf n Personen verteilt, so dass mindestens k Personen zum Rekonstruieren benötigt werden (sowas könnte man ein $((k, n)$ Schema nennen). Ist es möglich daraus

(a) ein $(k, n+1)$ Schema,

(b) ein $(k-1, n)$ Schema oder

(c) ein $(k+1, n)$ Schema zu machen,

ohne dass

(a) k Leute zusammenkommen und das Geheimnis rekonstruieren oder

(b) Leute ein neuen Teil des Geheimnisses zugewiesen bekommen.

(5 Punkte)

4. Aufgabe

Berechnet die Werte $p_{k,1}$ mit $k \in \{2, \ldots 16\}$.

(5 Punkte)