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

11. Übung Kryptographie

1. Aufgabe

(a) Sei p eine ungerade Primzahl und α ein Erzeuger der zyklischen Gruppe $\mathbb{Z}/p\mathbb{Z}^*$. Zeigt, dass dann entweder α oder $\alpha + p$ ein Erzeuger von $\mathbb{Z}/p^2\mathbb{Z}^*$ ist. (Ihr braucht nicht beweisen, dass $\mathbb{Z}/p^2\mathbb{Z}^*$ zyklisch ist)

(b) Findet einen Erzeuger von $\mathbb{Z}/29\mathbb{Z}^*$, der kein Erzeuger von $\mathbb{Z}/29^2\mathbb{Z}^*$ ist.

(5 Punkte)

2. Aufgabe

Gebt eine Formel für die Anzahl der ganzen Zahlen x mit $1 \leq x \leq n$ an, die

(a) über der Faktorbasis $B = \{2\}$ glatt sind.

(b) über der Faktorbasis $B = \{2, 3\}$ glatt sind.

Wieviele Prozent der ganze Zahlen zwischen 1 und 10000 sind also glatt über $B = \{2, 3\}$?

(5 Punkte)

3. Aufgabe

Führt einen Geburtstagsangriff auf den Kryptokurs durch, das heißt, findet heraus, ob zwei oder mehr Kursteilnehmer am selben Tag Geburtstag haben.

(1 Punkte)

4. Aufgabe

Schreibt ein quadratisches Sieb oder einen Random-Square-Faktorisierungsalgorithmus. Gebt ein paar Beispiele für Zahlen, die ihr faktorisiert habt an. Schreibt eine Probedivision. Gelingt es euch ein Beispiel zu finden, bei dem die Probedivision langsamer als eurer Algorithmus ist.

(9 Punkte)