Prof. Dr. A. Goerdt

TU Chemnitz
Wintersemester 2006/2007
22.01.2006

Datenschutz und Datensicherheit / Systemsicherheit

10. Übung

1. Aufgabe:

   a) Überlegen Sie sich noch einmal die Entsprechung (Isomorphie) von $\mathbb{Z}_{3\cdot 4\cdot 5} = \mathbb{Z}_{60}$ und $\mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_5$.

   b) Überlegen Sie sich, dass sich $\mathbb{Z}_4$ und $\mathbb{Z}_2 \times \mathbb{Z}_2$ nicht entsprechen.

   c) Sind $a_1, \ldots, a_n$ jeweils paarweise teilerfremd. Wieso ist ein Gleichungssystem

$$\begin{aligned} b_1 &\equiv x \mod a_1 \\ b_2 &\equiv x \mod a_2 \\ &\vdots \qquad\quad \vdots \\ b_n &\equiv x \mod a_n \end{aligned}$$

   eindeutig nach $x \in \mathbb{Z}_{a_1 \cdot \ldots \cdot a_n}$ lösbar?

2. Aufgabe:

   Ist g ein Generator von $\mathbb{Z}_n^*$. Geben Sie eine Entsprechung (Isomorphie) von $\mathbb{Z}_n^*$ und Multiplikation und $\mathbb{Z}_{\varphi(n)}$ und Addition an.

3. Aufgabe:

   a) Zahlen in denen ein Primteiler 2 mal d.h. als p^2 vorkommt, sind keine Carmichael Zahlen. Überlegen Sie sich das!

   b) Hat eine Zahl nur 2 verschiedene Primfaktoren, ist sie keine Carmichael-Zahl.

4. Aufgabe:

   Wenden Sie Miller-Rabin auf die Carmichael-Zahl 561 der Vorlesung an, um zu zeigen, dass diese keine Primzahl ist.

Bemerkung am Rande: Es gibt unendlich viele Carmichael Zahlen.