Kryptographie *WS 2015/16*
Barbara Baumeister
Tutoren: Apolonia Gottwald, Soeren Senkovic

6. Übungsblatt

Abgabe: Donnerstag, 3.12.2015

Aufgabe 1 Zeigen Sie mit dem Solovay-Strassen Test, dass n = 99991 mit einer Wahrscheinlichkeit von 75% eine Primzahl ist.

Aufgabe 2 Sei $n = 1703$ und $m = 1903$.

(a) Können n und m mit dem Faktorisierungsverfahren von Fermat in Primfaktoren zerlegt werden?

(b) Zerlegen Sie n und m mit der $p-1$-Methode von Pollard.

Aufgabe 3 (a) Sei $p \neq 2$ eine Primzahl. Beweisen Sie

$$\left(\frac{-1}{p}\right) = \begin{array}{rl} 1 & \text{falls } p \equiv 1 \pmod 4 \\ -1 & \text{falls } p \equiv 3 \pmod 4 \end{array}$$

(b) Beweisen Sie: Genau dann ist $n \in \mathbb{N}$ eine Primzahl, wenn die Kongruenz

$$(n-1)! \equiv -1 \pmod n$$

gilt.
Hinweis: Rechnen Sie in der Gruppe $\mathbb{Z}_n^*$.

Aufgabe 4 Es seien $a, b \in \mathbb{Z}$ und $n \in \mathbb{N}$. Zeigen Sie

(a) Die Kongruenz

$$ax \equiv b \pmod n$$

ist genau dann lösbar, wenn $d =$ggT(a, n) ein Teiler von b ist.

(b) Gilt $d \mid b$, so gibt es genau d Lösungen x zwischen 0 und $n-1$.