Universität Bielefeld

Peter Zeiner
Fakultät für Mathematik

Bielefeld, 29.11.2013

Wintersemester 2013/14

Elementare Zahlentheorie

Präsenzübungen 5

Aufgabe 1: $[3]_{17}$ ist eine primitive Restklasse. Berechnen Sie $\log_3 11 \pmod{17}$ auf verschiedene Arten, und diskutieren Sie deren Effizienz in diesem Fall.

Aufgabe 2: Zeigen Sie: $a(a^2-1)(a^2-4)$ ist durch 5 teilbar.

Aufgabe 3: Wählen Sie zwei Primzahlen $p, q > 30$ und kreieren Sie einen öffentlichen Schlüssel für das RSA-Verfahren. Geben Sie diesen Schlüssel Ihre{r,m} rechten Nachbar{in,n}. Verschlüsseln Sie eine Zahl m mit dem öffentlichen Schlüssel Ihre{r,s} linken Nachbar{in,n} und schicken Sie sie ih{r,m}.