Universität Bielefeld

Peter Zeiner
Fakultät für Mathematik

Bielefeld, 21.11.2013

Wintersemester 2013/14

Elementare Zahlentheorie

Übungszettel 6

Aufgabe 27: Bestimmen Sie alle primitiven Restklassen modulo 17. **(4 Punkte)**

Aufgabe 28: Zeigen Sie:

(a) Für beliebiges n gilt: $2730 \mid (n^{13} - n)$.

(b) $6^{30} - 6^{18} - 6^{12} + 1$ ist durch 247 teilbar. **(2+2 Punkte)**

Aufgabe 29: Sei p eine Primzahl und a kein Vielfaches von p. Welche Werte (modulo p) kann $a^{\frac{p-1}{2}}$ annehmen. *Hinweis:* Polynom, Körper. **(2 Punkte)**

Aufgabe 30: Betrachten Sie den Diffie-Hellman-Schlüsselaustausch. Ist jede Wahl von x, y sinnvoll? Skizzieren Sie kurz (!) mögliche Probleme. **(2 Punkte)**

Aufgabe 31: $[5]_{23}$ ist eine primitive Restklasse (mod 23). Berechnen Sie den diskreten Logarithmus $\log_5(3)$ mit Hilfe des Baby-step-giant-step-Verfahrens. **(4 Punkte)**

Abgabe bis zum 28.11.2013!