Universität Heidelberg
Mathematisches Institut

Dr. Rolf Busam
Andreas Riedel

Aufbau der Zahlsysteme

Sommersemester 2010

Aufgabenblatt 10 21. Juni 2010

Aufgabe 1. *(4 Punkte)*
Seien $m, n \in \mathbb{N},\ a, b \in \mathbb{Z}$. Zeigen Sie, dass das Kongruenzsystem

$$\begin{aligned} x &\equiv a \mod (m) \\ x &\equiv b \mod (n) \end{aligned}$$

genau dann lösbar ist, wenn $\mathrm{ggT}(m, n) \mid (a - b)$ gilt und die Lösungsmenge dann eine Restklasse mod $\mathrm{kgV}(m, n)$ ist.

Aufgabe 2. *(4 Punkte)*
Bestimmen Sie das kleinste Vielfache von 7, dass bei Division durch $2, 3, 4, 5, 6$ jeweils den Rest 1 lässt.

Aufgabe 3. *(4 Punkte)*
Zeigen Sie: Eine natürliche Zahl $n > 1$ ist genau dann eine Primzahl, wenn $(n-1)! \equiv -1 \mod (n)$ gilt.

Aufgabe 4. *(4 Punkte)*
Sei $p = 11, q = 13$ und $n = pq = 143$. Bestimmen Sie $\varphi(n)$ und ein $e > 1$ mit $1 < e < n$ und $\mathrm{ggT}(e, \varphi(n)) = 1$. Bestimmen Sie d mit $ed \equiv 1 \mod \varphi(n)$. Codieren Sie $x = 17$ mit der Funktion $E(x) = x^e$. Wie lautet die decodierte Zahl, wenn Sie als verschlüsselte Nachricht $y = 81$ erhalten, wobei Sie $n = 221$ und $e = 23$ als öffentlichen Schlüssel herausgegeben hatten?