Mathematisches Institut
der Universität München
Prof. Dr. O. Forster

SS 2009
17. Juli 2009

Algorithmische Zahlentheorie

Klausur

Aufgabe 1

Man berechne die Jacobi-Symbole $\left(\frac{-222}{1001}\right)$ und $\left(\frac{975}{1001}\right)$.

Aufgabe 2

Sei p eine Primzahl der Gestalt $p = 2q + 1$, wobei q ebenfalls prim sei. Man zeige:

$$g := -2 \equiv p - 2$$

ist genau dann Primitivwurzel modulo p, wenn $p \equiv 5, 7 \bmod 8$.

Aufgabe 3

Alice verwendet beim Aufstellen ihres RSA-Systems statt Primzahlen teilerfremde Carmichaelzahlen p, q, setzt $N := pq$ und bestimmt Verschlüsselungs- und Entschlüsselungs-Exponenten e bzw. d durch die Kongruenz

$$ed \equiv 1 \bmod (p-1)(q-1).$$

a) Man zeige, dass gilt: $x^{ed} \equiv x \bmod N$ für alle $x \in (\mathbb{Z}/N)^*$.

b) Gilt $x^{ed} \equiv x \bmod N$ sogar für alle $x \in \mathbb{Z}/N$?

Aufgabe 4

Sei p eine ungerade Primzahl und seien g, h zwei Primitivwurzeln modulo p. Man beweise:

$$\log_g(h) \log_h(g) \equiv 1 \bmod (p-1).$$

Aufgabe 5 Der Körper $\mathbb{F}_8$ werde dargestellt als

$$\mathbb{F}_8 = \mathbb{F}_2[X]/(\phi(X)) \quad \text{mit} \quad \phi(X) := X^3 + X + 1.$$

Die Elemente von $\mathbb{F}_8$ seien mit Bitvektoren der Länge 3 identifiziert, wobei dem Körperelement $\xi = \sum_{i=0}^{2} b_i X^i \bmod \phi(X)$ der Bitvektor $(b_2 b_1 b_0)$ zugeordnet sei. Diese Bitvektoren seien durch die Zahlen $x = 0, 1, \ldots, 7$ bezeichnet, wobei $x = \sum_{i=0}^{2} b_i 2^i$.

a) Man zeige: Die Abbildung $E : \mathbb{F}_8 \to \mathbb{F}_8,\ x \mapsto x^2 + 1$ ist bijektiv.

b) Die Funktion E werde als Block-Verschlüsselung für Blöcke der Bitlänge 3 aufgefasst. Man verschlüssele den Text

$$\texttt{4711} \in (\mathbb{F}_8)^4$$

im CBC-Modus mit Initialisierungs-Vektor $iv = \texttt{5}$.