Algebra für Lehramtskandidaten

SS 2005 Peter Schmitt *Aufgaben für den 6. bzw. 7. Juni*

Außerdem noch offen: (40) am Montag, sowie (45) und (46) am Dienstag.

Abelsche Gruppen und ihre Struktur

(43b) *(Ordnung in zyklischen Gruppen)*
Zeige: Es gilt $\operatorname{ord}(g^n) = \frac{\operatorname{ord} g}{(\operatorname{ord} g, n)} = \frac{[\operatorname{ord} g, n]}{n}$.

zahlentheoretische Funktionen

(47) *(Faltung)*
Zeige: Die Faltung zahlentheoretischer Funktionen ist assoziativ.

(48) *(Möbiussche Umkehrformel)*
Rechne nach: Die Möbiussche Umkehrfunktion μ ist bezüglich der Faltung zur 1-Funktion invers.

(49) *(Eulersche φ-Funktion)*
Berechne die Summenfunktion der φ-Funktion.

(50*) *(Chinesischer Restsatz)*
Löse die die folgenden simultanen Kongruenzen: $3x \equiv 5(7), 5x \equiv 4(11), 4x \equiv 9(13)$

(51*) *(Chinesischer Restsatz)*
Löse $x^3 \equiv 1 \bmod 945$.

(52*) *(RSA-Verschlüsselung)*
Die folgende Nachricht wurde mittels $x^3 \bmod 187$ verschlüsselt. Wie lautet sie *(sofern richtig gerechnet wurde :-)*?
104, 35, 115, 52, 131 40
(A=18,...,Z=47 – prime Restklassen)

(53) *(RSA-Verschlüsselung)*
Erkläre: Wenn dieselbe Nachricht m mittels $c_i(m) \equiv x^3 \bmod K_i$ $(i = 1, 2, 3)$ für drei Empfänger mit verschiedenen K_i verschlüsselt wurde, so kann sie aus diesen drei Nachrichten leicht ermittelt werden:
Bestimme $x^3 \bmod K_1K_2K_3$ (und ziehe die Wurzel)!