

Algebra für Lehramtskandidaten

SS 2005 Peter Schmitt

Aufgaben für den 13. bzw. 14. Juni

Abelsche Gruppen und ihre Struktur

(43b) (*Ordnung in zyklischen Gruppen*)

Zeige: Es gilt $\text{ord}(g^n) = \frac{\text{ord } g}{(\text{ord } g, n)} = \frac{[\text{ord } g, n]}{n}$.

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 $x^3 \equiv 1 \pmod{945}$.

(52*) (*RSA-Verschlüsselung*)

Die folgende Nachricht wurde mittels $x^3 \pmod{187}$ verschlüsselt. Wie lautet sie (*sofern richtig gerechnet wurde :-*)?

104, 35, **72**, 52, **48**, 40

(A=18, ..., Z=47 – prime Restklassen)

(53) (*RSA-Verschlüsselung*)

Erkläre: Wenn dieselbe Nachricht m mittels $c_i(m) \equiv x^3 \pmod{K_i}$ ($i = 1, 2, 3$) für drei Empfänger mit verschiedenen K_i verschlüsselt wurde, so kann sie aus diesen drei Nachrichten leicht ermittelt werden:

Bestimme $x^3 \pmod{K_1 K_2 K_3}$ (und ziehe die Wurzel)!

(54*) (*Quadratische Reste*)

(a) Ist $2^8 + 1$ quadratischer Rest modulo $2^{16} + 1$?

(55*) (*Jacobi-Symbol*)

(a) Berechne $\frac{(1665)}{(2431)}$.

(b) Ist 1665 quadratischer Rest modulo 2431?

(56*) (*Münzwurf per Telephon*)

A wählt 83 und 571 als Primzahlen und **B** die Zahl 25166.

A wählt „+“. Hat er gewonnen?

(57*) (*Münzwurf per Telephon*)

A nennt $n = 3397$, **B** nennt $y = 2380$.

Bereite **B** darauf vor, den Losentscheid auf jeden Fall zu gewinnen.