Algebra für Lehramtskandidaten

SS 2005 Peter Schmitt *Aufgaben für den 20. bzw. 21. Juni*

Vorzubereiten sind jeweils die noch nicht vollständig gerechneten Beispiele.

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

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

(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, **72**, 52, **48**, 40
(A=18,...,Z=47 – prime Restklassen)

(53) *(RSA-Verschlüsselung)*
Erkläre: Wenn dieselbe Nachricht m mittels $c_i(m) \equiv x^3 \bmod K_i$ $(i = 1, 2, 3)$ 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)!

(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.
(*Rechenhilfe:* Eine der Quadratwurzeln aus y ist kongruent zu 12 bzw 22 modulo den Primfaktoren von n.)

(58) *(Faltung)*
Zeige: Zu jeder nicht-verschwindenden multiplikativen zahlentheoretischen Funktion gibt es eine bezüglich der Faltung inverse Funktion.

Ringe

(59) *(Axiome)*
Zeige: In jedem Ring gilt $0 \cdot 0 = 0$.

(60) *(Quotientenkörper)*
Konstruiere *(analog zur Konstruktion des Quotientenkörpers)* die ganzen Zahlen aus den natürlichen Zahlen.
Welche Eigenschaften der natürlichen Zahlen werden dabei verwendet?