Diskrete Mathematik

Blatt 6, 27.05.2010, Abgabe 07.06.2010, 10.10 Uhr

Aufgabe 1. Zeige: N ist Carmichael-Zahl gdw $N = p_1 \cdots p_r$ Produkt von $r \geq 3$ verschiedene Primzahlen $p_1, \ldots, p_r$ ist, so dass $(p_j - 1) \mid (\frac{N}{p_j} - 1)$ für $j = 1, \ldots, r$.

Hinweis: Satz 4.12 (Skript)

Eine **Blum-Zahl** ist ein RSA–Modul $N = pq$ mit p, q prim und $p, q = 3 \bmod 4$.

Aufgabe 2: Zeigen Sie, dass die folgenden Aussagen äquivalent sind:

1. $G = (V, E)$ ist ein Baum
2. G ist maximal kreisfrei, d.h. G ist kreisfrei und für jede Kante $e \in \{\{v_1, v_2\}, v_1, v_2 \in V\} \backslash E$ hat der Graph $(V, E \cup \{e\})$ einen Kreis.
3. G ist minimal zusammenhängend, d.h. G ist zusammenhängend und für jede Kante $e \in E$ ist $(V, E \backslash \{e\})$ nicht zusammenhängend.

Aufgabe 3. *Ganze Gauß'sche Zahlen.* Zeigen Sie, dass $\mathbb{Z}[i] := \{a + bi : a, b \in \mathbb{Z}\}$ mit $i^2 = -1$ ein kommutativer Ring mit Einselement ist und dass genau vier Elemente von $\mathbb{Z}[i]$ ein multiplikatives Inverses besitzen. Ist $\mathbb{Z}[i]$ ein Integritätsbereich?

Aufgabe 4. Sei G endliche, abelsche Gruppe, $a, b \in G$. Zeige:

1. $\mathrm{ggT}(\mathrm{ord}(a), \mathrm{ord}(b)) = 1$ impliziert $\mathrm{ord}(a \cdot b) = \mathrm{ord}(a) \cdot \mathrm{ord}(b)$.

2. $\mathrm{kgv}(\mathrm{ord}(a) \mid a \in G) = \max\{\mathrm{ord}(a) \mid a \in G\}$.

Hinweis: Lemma 4.4, Korollar 4.5 Skript Schnorr

6 Punkte pro Aufgabe