Prof. Klaus Mohnke
Institut für Mathematik
Rudower Chaussee 25
Haus 1 Raum 306

Übungsblatt 10

Lineare Algebra und Analytische Geometrie I WS 2010/11

Abgabe: 17.1.2011, Besprechung: 17.1.-20.1., Test: 24.1.-27.1.

Aufgabe 1. Gegeben Sei der öffentliche RSA-Schlüssel $n = 21$ und $b = 5$. Bestimmen Sie a, p und q. Entschlüsseln Sie dann die (verschlüsselte) Nachricht $y = 13$.

Aufgabe 2. (a) Sei p eine Primzahl und a eine natürliche Zahl. Beweisen Sie mittels Induktion über a, dass die Gleichung

$$a^p = a \mod p$$

erfüllt ist.
(b) Seien zusätzlich a und p teilerfremd. Folgern Sie aus (a), dass die Gleichung

$$a^{p-1} = 1 \mod p$$

erfüllt ist.
Benutzen Sie beides Mal nicht den Satz von Fermat oder Euler.

Aufgabe 3. Schreiben Sie die folgenden komplexen Zahlen in der Form $a + b\mathrm{i}$ mit $a, b \in \mathbb{R}$:

$$\frac{(1+2\mathrm{i})(1-\mathrm{i})}{(1+\mathrm{i})^2}, \quad \frac{|2+\mathrm{i}|(1-2\mathrm{i})}{\overline{(1+\mathrm{i})}(3+\mathrm{i})}$$

Aufgabe 4. (a) Betrachten Sie folgende Relation $\sim$ auf der Menge $\mathbb{Z} \times (\mathbb{Z}\backslash\{0\})$: $(a, b) \sim (c, d) \Leftrightarrow ad = bc$. Zeigen Sie, dass dies eine Äquivalenzrelation ist. Im Folgenden werden die Äquivalenzklassen mit $[(a, b)]$ und der Quotient $\mathbb{Z} \times (\mathbb{Z}\backslash\{0\})/\sim$ mit $\mathbb{Q}$ bezeichnet.
(b) Auf $\mathbb{Q}$ werden zwei binäre Operatonen definiert:

$$[(a, b)] + [(c, d)] := [(ad + bc, bd)]$$
$$[(a, b)] \cdot [(c, d)] := [(ac, bd)].$$

Beweisen Sie, dass diese wohldefiniert sind, d.h. dass sie nicht von der Wahl des Repräsentanten, (a, b), der Äquivalenzklasse, $[(a, b)]$, abhängen.
(c) Sie kennen die Äquivalenzklasse $[(a, b)]$ bereits als *Bruch* aus der Schule:

$$\frac{a}{b} := [(a, b)].$$

Überzeugen Sie sich davon, indem Sie die Operationen unter (b) in dieser Schreibweise notieren!
(d) Zeigen Sie, dass $(\mathbb{Q}, +, \cdot)$ ein Körper ist. Bestimmen Sie das Nullelement, das Einselement, das additive und das multiplikative Inverse.