Übungsblatt 4

Hertrampf, Mattes
FMI/TI, FMI/ALG
Universität Stuttgart

Aufgabe 1: Euklidischer Algorithmus **[10]**

Berechnen Sie den größten gemeinsamen Teiler der folgenden Zahlen mit dem euklidischen Algorithmus.
Wenden Sie das Lemma von Bézout an, um den ggT(a, b) in der Form $am + bn$ darzustellen.
Hinweis: Folgen Sie dem Beweis des Lemmas von Bézout.

(a) ggT(44,126)
(b) ggT(33,117)
(c) ggT(19,98)
(d) ggT(27,113) [P]

Aufgabe 2: Restklassenringe **[15]**

(a) Stellen Sie eine Additions- und Multiplikationstabelle für die folgenden Restklassenringe auf. Geben Sie jeweils die multiplikativ invertierbaren Elemente und ihre jeweiligen Inversen an.
(i) $\mathbb{Z}/8\mathbb{Z}$
(ii) $\mathbb{Z}/5\mathbb{Z}$
Hinweis: Die Operationen sind jeweils kommutativ.

(b) In der Vorlesung wurde die Relation $\equiv (\mod n)$ durch

$$k \equiv l \mod n \iff k \in l + n\mathbb{Z} \tag{1}$$

definiert. Die Menge $k + n\mathbb{Z}$ war dabei definiert als die Menge

$$k + n\mathbb{Z} = \{..., k - 2n, k - n, k, k + n, k + 2n, k + 3n, ...\} \tag{2}$$

Zeigen Sie, dass diese Relation tatsächlich eine Äquivalenzrelation ist, also dass sie reflexiv, transitiv und symmetrisch ist.

Aufgabe 3: Chinesischer Restsatz **[15]**

(A)[P] Geben Sie die Abbildung $\mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $(x+4\mathbb{Z}) \mapsto (x+2\mathbb{Z}, x+2\mathbb{Z})$an. Woran erkennt man, dass diese nicht bijektiv ist?

(a) Warum existiert ein Isomorphismus von $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \mapsto \mathbb{Z}/12\mathbb{Z}$? Geben Sie einen solchen Homomorphismus mittels einer Wertetabelle an.

(b) Lösen Sie die folgenden Systeme von Kongruenzen:

(i)

$$x \equiv 2 \mod 3$$
$$x \equiv 1 \bmod 2$$
$$x \equiv 2 \bmod 5$$

(ii)

$$\begin{aligned} 2x &\equiv 0 \bmod 2 \\ x &\equiv 2 \bmod 4 \\ x &\equiv 3 \bmod 5 \\ x &\equiv 3 \bmod 7 \end{aligned}$$

(iii)

$$\begin{aligned} 7x &\equiv 1 \bmod 10 \\ x - 4 &\equiv 5 \bmod 6 \\ 3x &\equiv 0 \bmod 9 \end{aligned}$$

(iv) [P]

$$\begin{aligned} x &\equiv 1 \bmod 4 \\ x &\equiv 3 \bmod 5 \\ x &\equiv 2 \bmod 7 \end{aligned}$$

Aufgabe 4: Satz von Fermat **[10]**

Sei p eine ungerade Primzahl. Zeigen Sie für alle $a \in \mathbb{Z}$: $a^p \equiv a \mod 2p$.

Aufgabe 5: Kongruenzen in Monoiden [P] **[0]**

Sei M ein Monoid und $R \subseteq M \times M$ eine binäre Relation darüber. In diesem Zusammenhang ist es üblich $s\ R\ t$ statt $(s,t) \in R$ zu schreiben.

Eine solche Relation R heißt *Kongruenz*, wenn R eine Äquivalenzrelation (also reflexiv, transitiv und symmetrisch) ist und außerdem $s\ R\ s'$ und $t\ R\ t'$ für alle $s, s', t, t' \in M$ impliziert, dass $st\ R\ s't'$ gilt.

Mit $[s]_R$ (oder kurz $[s]$) bezeichnen wir die Äquivalenzklasse von s:

$$[s]_R = \{t \in M \mid s\ R\ t\}$$

Ferner bezeichnen wir mit M/R die Menge aller Äquivalenzklassen von R:

$$M/R = \{[s]_R \mid s \in M\}$$

Schließlich definieren wir auf M/R folgende Verknüpfung:

$$[s]_R[t]_R = [st]_R$$

(a) **Zeigen Sie:** Diese Verknüpfung ist wohldefiniert (d. h. das Ergebnis der Verknüpfung ist eindeutig festgelegt).

(b) **Zeigen Sie:** M/R bildet mit obiger Verknüpfung ein Monoid.

Sei $\Sigma = \{a, b\}$ und bezeichne Σ^* das Monoid der endlichen Wörter über Σ mit Konkatenation als Verknüpfung (genauer: Σ^* ist das *freie Monoid* über Σ). Das neutrale Element von Σ^* ist dann das leere Wort, das wir mir ε bezeichnen.

Für ein Wort $w \in \Sigma^*$ bezeichne $|w|_a$ die Anzahl der Vorkommen von a in w und $|w|_b$ die von b.

Damit definieren wir auf Σ^* die Relation $\sim \subseteq \Sigma^* \times \Sigma^*$ über

$$u \sim v \iff |u|_a = |v|_a \text{ und } |u|_b = |v|_b.$$

(c) **Zeigen Sie:** $\sim$ ist eine Kongruenz.

Die Menge der natürlichen Zahlen $\mathbb{N} = \{0, 1, \dots\}$ bildet mit der Addition als Verknüpfung ebenfalls ein Monoid. Mit $\mathbb{N}^2$ bezeichnen wir das direkte Produkt dieses Monoids mit sich selbst, d. h. das Monoid, dessen Element Paare natürlicher Zahlen sind, mit der Verknüpfung

$$(m, n)(m', n') = (m + m', n + n').$$

(d) **Zeigen Sie:** $\Sigma^*/\sim$ ist isomorph zu $\mathbb{N}^2$.