Challenge!

Seien $a_1, a_2, \ldots, a_n \in \mathbb{Z}$. Gebe einen $\mathcal{O}(n^2)$ Algorithmus an, der eine zusammenhängende Teilfolge $a_i, a_{i+1}, \ldots, a_j$ findet mit $1 \leq i \leq j \leq n$, so dass $n \mid (a_i + a_{i+1} + \ldots + a_j)$.
Eine genaue Laufzeitanalyse vom angegebenem Algorithmus ist nicht nötig.

Tipp: Betrachte die Summen $S_i := \sum_{k=1}^{i} a_k$ für $1 \leq i \leq n$.

Monoid-/Gruppeneigenschaften überprüfen

Für jede der folgenden Algebren, entscheide ob sie ein Monoid, eine Gruppe oder keines davon ist:

- $\langle \mathbb{Z}; - \rangle$
- $\langle \mathcal{P}(\mathbb{N}); \cap \rangle$

Monoid-/Gruppeneigenschaften überprüfen

Für jede der folgenden Algebren, entscheide ob sie ein Monoid, eine Gruppe oder keines davon ist:

- $\langle \mathbb{Z}; - \rangle$
- $\langle \mathcal{P}(\mathbb{N}); \cap \rangle$

Das heisst, überprüfe

1. Ist die Operation assoziativ?
2. Gibt es ein neutrales Element?

Falls 1 oder 2 scheitert, dann sind wir fertig.

Monoid-/Gruppeneigenschaften überprüfen

Für jede der folgenden Algebren, entscheide ob sie ein Monoid, eine Gruppe oder keines davon ist:

- $\langle \mathbb{Z}; - \rangle$
- $\langle \mathcal{P}(\mathbb{N}); \cap \rangle$

Das heisst, überprüfe

1. Ist die Operation assoziativ?
2. Gibt es ein neutrales Element?

Falls 1 oder 2 scheitert, dann sind wir fertig.

Sonst haben wir schon ein Monoid. Dann bleibt noch zu überprüfen

3. Besitzt jedes Element ein Inverses?

Subgroups

Let $\langle G; *, \hat{}, e \rangle$ be a group and define

$$H = \{a \in G \mid \forall b \in G \; a * b = b * a\}$$

(i.e. all commutative elements of G). Prove that H is a subgroup of G.

Subgroups

Let $\langle G; *, \hat{}, e \rangle$ be a group and define

$$H = \{a \in G \mid \forall b \in G \; a * b = b * a\}$$

(i.e. all commutative elements of G). Prove that H is a subgroup of G.

Das heisst, wir müssen zeigen für alle $a, b \in H$

1. $e \in H$
2. $a * b \in H$ (Operationen in H bleiben auch in H, H ist *abgeschlossen* (*closed*) bezüglich $*$)
3. $\hat{a} \in H$ (H abgeschlossen bezüglich $\hat{}$)

Mehr Subgroups

Let H, H' subgroups of G. Prove

$$H \cup H' \text{ is a subgroup of } G \implies H \subseteq H' \text{ or } H' \subseteq H.$$

Mehr Subgroups

Let H, H' subgroups of G. Prove

$$H \cup H' \text{ is a subgroup of } G \implies H \subseteq H' \text{ or } H' \subseteq H.$$

Trick: Aussagen der Form "S oder T" kann man beweisen, indem man "nicht $S \implies T$" beweist.

Nützliche Tatsache

Beweise:

$$g \text{ ist ein “generator” von } \langle \mathbb{Z}_n; \oplus \rangle \iff \gcd(n, g) = 1.$$

Folgendes könnte dabei hilfreich sein

$$\operatorname{lcm}(a, b) \cdot \gcd(a, b) = a \cdot b.$$

Definition (Ordnung)

Sei G eine Gruppe und $a \in G$. Dann ist $\text{ord}(a)$ das kleinte $m \geq 1$, so dass $a^m = e$.

Definition (Ordnung)

Sei G eine Gruppe und $a \in G$. Dann ist $\text{ord}(a)$ das kleinte $m \geq 1$, so dass $a^m = e$.

Lemma

$\langle a \rangle = \{e, a, a^2, \ldots, a^{\text{ord}(a)-1}\}$ *ist die kleinste Subgroup mit* a.

Definition (Ordnung)

Sei G eine Gruppe und $a \in G$. Dann ist $\text{ord}(a)$ das kleinte $m \geq 1$, so dass $a^m = e$.

Lemma

$\langle a \rangle = \{e, a, a^2, \ldots, a^{\text{ord}(a)-1}\}$ *ist die kleinste Subgroup mit* a.

Theorem (Lagrange)

Sei H *ein Subgroup von* G. *Dann gilt* $|H| \mid |G|$.

Definition (Ordnung)

Sei G eine Gruppe und $a \in G$. Dann ist $\text{ord}(a)$ das kleinte $m \geq 1$, so dass $a^m = e$.

Lemma

$\langle a \rangle = \{e, a, a^2, \ldots, a^{\text{ord}(a)-1}\}$ *ist die kleinste Subgroup mit* a.

Theorem (Lagrange)

Sei H *ein Subgroup von* G. *Dann gilt* $|H| \mid |G|$.

Lemma

Für alle $a \in G$ *gilt:* $\text{ord}(a) \mid G$.

Definition (Ordnung)

Sei G eine Gruppe und $a \in G$. Dann ist $\text{ord}(a)$ das kleinte $m \geq 1$, so dass $a^m = e$.

Lemma

$\langle a \rangle = \{e, a, a^2, \ldots, a^{\text{ord}(a)-1}\}$ *ist die kleinste Subgroup mit* a.

Theorem (Lagrange)

Sei H *ein Subgroup von* G. *Dann gilt* $|H| \mid |G|$.

Lemma

Für alle $a \in G$ *gilt:* $\text{ord}(a) \mid G$.

Lemma

Für alle $a \in G$ *gilt:* $a^{|G|} = e$.

Next Level nützliche Tatsache

Lemma

Sei g_1 ein Generator von $\mathbb{Z}_m$ und g_2 ein Generator von $\mathbb{Z}_n$. Dann gilt

$$\gcd(m, n) = 1 \iff (g_1, g_2) \text{ ein Generator von } \langle \mathbb{Z}_m; \oplus \rangle \times \langle \mathbb{Z}_n; \oplus \rangle.$$

Beweisidee (eine Richtung)

Wir beweisen eine abgeschwächte Form davon:

$$\gcd(m, n) = 1 \implies \langle (1, 1) \rangle = \langle \mathbb{Z}_m; \oplus \rangle \times \langle \mathbb{Z}_n; \oplus \rangle$$

Wieder Subgroups

Liste alle Subgroups von $\langle \mathbb{Z}_3; \oplus \rangle \times \langle \mathbb{Z}_4; \oplus \rangle$ auf.