Organisatorisches

- DiMa für Master of Science Mathe anrechenbar
- Korrigierte Version von Aufgabe 6.4 im Netz
  - 1234*x = 110 (mod 654321)
- Klausurtermin
  - Bekanntgabe im Dezember

Wiederholung

- Laufzeit Euklidischer Algorithmus
  - wc Laufzeit bei Fibonaccizahlen
  - $\mathcal{O}(\log^2(\max\{a,b\}))$
- Erweiterter Euklidischer Algorithmus (EEA)
  - Berechnet x,y mit ggT(a,b) = ax + by
- Abelsche Gruppen
  - $(\mathbb{Z}_m, +)$
  - $(\mathbb{Z}_n^*, *)$

Bsp.: nicht-abelsche Gruppe

Symmetrische Gruppe $\mathcal{G}_n := \{\pi_n \mid \pi_n \text{ ist Permutation auf } [n]\}$

Satz: ($\mathcal{G}_N$, $\circ$) mit $\circ$: $\pi \circ \pi' = \pi(\pi')$ ist eine (nicht-kommutative) Gruppe.

- Abgeschlossenheit:
  - $\pi(\pi')$ ist eine Permutation
- Assoziativität:
  - $\pi\circ(\pi'\circ\pi'') = \pi\circ(\pi'(\pi'')) = \pi(\pi'(\pi'')) = \pi(\pi')\circ\pi'' = (\pi\circ\pi')\circ\pi''$
- Neutrales Element: Identität id: [n] $\rightarrow$ [n]
- Inverses Element:

$$\pi = \begin{pmatrix} 1 & 2 & \dots & n \\ \pi(1) & \pi(2) & \dots & \pi(n) \end{pmatrix},\ \pi^{-1} = \begin{pmatrix} \pi(1) & \pi(2) & \dots & \pi(n) \\ 1 & 2 & \dots & n \end{pmatrix}$$

- Nicht kommutativ (d.h. nicht-abelsch):

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

Lösbarkeit von linearen Gleichungen

Satz: Sei $n \in \mathbb{N}$ und $a \in \mathbb{Z}$ teilerfremd zu n. Dann besitzt die lineare Gleichung

$$ax = b \bmod n$$

für jedes $b \in \mathbb{Z}_n$ genau eine Lösung $x \in \mathbb{Z}_n$.

Existenz:

- Berechne EEA Koeffizienten x‘,y‘ mit ax‘+ny‘ = 1.
- Setze $a^{-1} = x' \bmod n \in \mathbb{Z}_n^*$.

  $\Rightarrow x = a^{-1}b \bmod n$

Eindeutigkeit:

- Abbildung $f: \mathbb{Z}_n \mapsto \mathbb{Z}_n$, $b \mapsto a^{-1}b \bmod n$ ist bijektiv.
  - Inverse Abbildung f^{-1}: $f: \mathbb{Z}_n \mapsto \mathbb{Z}_n$, $x \mapsto ax \bmod n$

Gleichheitsregel: Für jedes $a \in \mathbb{Z}_n^*$: $\{a^{-1}b=f(b) \mid b \in \mathbb{Z}_n\} = \mathbb{Z}_n$

Ordnung einer Gruppe

Def: Sei G eine multiplikative endliche Gruppe mit neutralem Element 1.

- Ordnung der Gruppe: ord(G) := |G|
- Ordnung eines Elements $a \in G$: $ord_G(a) := \min\{i \in \mathbb{N} \mid a^i = 1\}$
- $H \subseteq G$ ist Untergruppe $\Leftrightarrow$ H erfüllt Gruppeneigenschaften
- $\langle a \rangle = \{a, a^2, a^3, \ldots, a^{ord_G(a)}\}$ ist die von a erzeugte Untergruppe.
  - Von einem Element a erzeugte Untergruppen heißen zyklisch.
  - a heisst Generator (oder primitives Element) der Untergruppe.

Bsp: Betrachten die multiplikative Gruppe $G=\mathbb{Z}_7^*$.

- $ord(\mathbb{Z}_7^*) = ord(\{1,2,\ldots,6\}) = 6$
- $ord_G(4) = 3$, denn $4^1=4$, $4^2=2$, $4^3=1$
- $H=\{1,2,4\}$ ist Untergruppe: $2*4=1$, d.h. $2^{-1}=4$ und $4^{-1}=2$.
- $H=\langle 4 \rangle$ ist zyklische Untergruppe der Ordnung 3 mit Generatoren 2,4.
- $G=\langle 3 \rangle$ ist ebenfalls zyklisch

Satz von Euler

Satz von Euler: Sei G eine multiplikative Gruppe mit neutralem Element 1. Dann gilt für alle $a \in G$:

$$\mathbf{a^{|G|} = 1.}$$

- Sei $G=\{g_1,\ldots,g_n\}$.
- Betrachten bijektive Abbildung $f: G \to G,\ g \mapsto ag$.
- Gleichheitsregel: $\{g_1,\ldots,g_n\} = \{ag_1,\ldots,ag_n\}$

$$\Rightarrow \prod_{i=1}^{n} g_i = \prod_{i=1}^{n} ag_i = a^n \prod_{i=1}^{n} g_i$$

$$\Rightarrow a^n = a^{|G|} = 1$$

Elementordnung in endlichen Gruppen

Satz: Sei G eine endliche Gruppe. Dann gilt für alle $a \in G$:
$ord_G(a) \leq ord(G)$.

- Ann.: Sei a ein Element mit $k = ord_G(a) \geq |G|+1$
- Betrachten Abb.: $[k] \rightarrow G$, $i \mapsto a^i$
- Schubfachprinzip:
  - $\exists\ 1 \leq i < j \leq k: a^i = a^j \in G$.
- Multiplikation mit $(a^{-1})^i$ liefert:
  - $1 = a^{j-i}$ mit $0 < j-i < k$.
    $\Rightarrow ord_G(a) < k$ (Widerspruch)

Elementordnung teilt Gruppenordnung

Satz: Sei G eine Gruppe. Dann gilt für alle a $\in$ G:
$ord_G(a) \mid ord(G)$.

Ann: $ord_G(a) \nmid ord(G)$

- Division mit Rest:
  - $ord(G) = q*ord_G(a) + r$ mit $0 < r < ord_G(a)$
- Es gilt
  - $a^r = a^{ord(G)-q*ord_G(a)} = (a^{ord(G)})*(a^{ord_G(a)})^{-q} = 1*(1^q)^{-1} = 1.$

  (Widerspruch zur Minimalität von $ord_G(a)$)

Nebenklassen von Untergruppen

Def: Sei G abelsch, H Untergruppe von G. Für jedes b $\in$ G ist
b$\circ$H = {b$\circ$h | h $\in$ H}
eine Nebenklasse von b.

Bsp.:
G = ($\mathbb{Z}_8$, +)

- H = {0,4}
- 1+H = {1,5}, 2+H={2,6}, 3+H={3,7}, 4+H=H

G = ($\mathbb{Z}_7^*$,*)

- H = {1,2,4} ist Untergruppe.
- 3H = {3,6,5}, 2H={2,4,1}=H

Eigenschaften von Nebenklassen

Satz: Sei G endlich, abelsch und H Untergruppe von G.

1. **$h \circ H = H$ für alle $h \in H$**
2. **Für $a,b \in G$: $a \circ H = b \circ H$ oder $a \circ H \cap b \circ H = \emptyset$**
3. **$|a \circ H| = |H|$ für alle $a \in G$**
4. **Die Nebenklassen $a \circ H$, $a \in G$ von H partitionieren G.**

zu 1.:

- Abgeschlossenheit von H: $h \circ H \subseteq H$
- Sei $g \in H$: $g = e \circ g = h \circ (h^{-1} \circ g) \in h \circ H$

zu 2.:

- Seien $a,b \in G$ mit $a \circ H \cap b \circ H \neq \emptyset$, d.h. $\exists\, h_1, h_2$: $a \circ h_1 = b \circ h_2$
  $\Rightarrow a \circ H = (b \circ h_1^{-1} \circ h_2)\, H = b \circ (h_1^{-1} \circ h_2 \circ H) = b \circ H$

zu 3.:

- Abb.: $H \rightarrow a \circ H$, $h \mapsto a \circ h$ ist Bijektion in G.
  $\Rightarrow |H| = |a \circ H|$ (Gleichheitsregel)

zu 4.:

- Wegen $e \in H$ gilt $a \in a \circ H$ für alle $a \in G$. Daher: $G \subseteq \cup_{a \in G}\, a \circ H \subseteq G$.
- Wegen 3. bilden die Nebenklassen $a \circ H$ eine Partition von H.

Untergruppenordnung teilt Gruppenordnung

Def.: Sei G endlich, abelsch, H Untergruppe von G.

- **G/H = Menge der verschiedenen Nebenklassen von H in G**
- **$ind_G(H) = |G/H|$ (alternative Notation [G:H])**

Satz von Lagrange: Sei G endlich, abelsch und H eine Untergruppe von G. Dann gilt:

$|G| = |H| * ind_G(H)$, insbesondere gilt $ord_G(H) \mid ord(G)$.

- Alle Nebenklassen besitzen gleiche Kardinalität |H|.
- Es gibt $ind_G(H)$ viele verschiedene Nebenklassen H von G.
- Alle Nebenklassen bilden eine Partition von G.

Die Faktorgruppe G/H

Satz: Sei G eine (multiplikative) Gruppe. Dann ist (G/H,*) eine Gruppe, die sogenannte Faktorgruppe.

- Abgeschlossenheit: *: $G/H \times G/H \to G/H$, $(aH,bH) \mapsto abH$
  - Repräsentanten-Unabhängigkeit:
    z.z.: $aH=a'H$ und $bH=b'H \Rightarrow abH = a'b'H$
  - Es gilt $a \in aH=a'H \Rightarrow \exists\, h_1 \in H$: $a=a'h_1$, analog $\exists\, h_2 \in H$: $b=b'h_2$
    $\Rightarrow abH = (a'h_1\, b'h_2)\, H = a'b'\, (h_1h_2\, H) = a'b'H$

- Neutrales Element: H
- Inverses zu aH: $a^{-1}H$, wobei a^{-1} Inverses von a in G.

Bsp: $\mathbb{Z}_7^*$ mit $H_1=H=2H=4H=\{1,2,4\}$, $H_2=3H=5H=6H=\{3,5,6\}$

- H_1 ist neutrales Element: $H_1*H_1=H_1$ und $H_1*H_2=H_2$
  - $h_1*h_1 \in H_1$, $h_1*h_2 \in H_2$ für alle $h_1 \in H_1$, $h_2 \in H_2$
- $(H_2)^{-1} = H_2$: $H_2*H_2 = H_1$
  - $h_2*h_2' \in H_1$ für alle $h_2, h_2' \in H_2$

Isomorphismus

Def: Seien (G,+), (G‘,*) Gruppen. Man nennt
f: G $\rightarrow$ G‘ einen Isomorphismus falls

1. **f ist bijektiv**
2. **f(u+v) = f(u) * f(v) für alle u,v$\in$G**
   (f ist Homomorphismus)

- G und G‘ sind isomorph $\Leftrightarrow \exists$ Isomorphismus f: G $\rightarrow$ G‘
- Notation: G $\cong$ G‘

Jede zykl. Gruppe ist isomorph zu $(\mathbb{Z}_m,+)$

Satz: Sei G eine zyklische Gruppe mit Ordnung m. Dann ist $G \cong (\mathbb{Z}_m,+)$.

- Es gibt Generator a mit $G=\{a^i \mid i \in [m]\}$.
- Betrachten $f: \mathbb{Z}_m \to G$, $i \mapsto a^i$.
- Bijektivität von f:
  - f surjektiv wegen $G=\{a^i \mid i \in [m]\}$ und $|G|=|\mathbb{Z}_m|$.
- f Homomorphismus:
  - $f(i+j) = a^{i+j} = a^i * a^j = f(i) * f(j)$ für alle $i,j \in \mathbb{Z}_m$

Diskreter Logarithmus Problem

DLP (Diskreter Logarithmus Problem)

- **Gegeben: G, a Generator in g, b = <a>**
- **Gesucht: i $\in \mathbb{Z}_{|G|}$ mit $a^i = b$**

- Betrachten Isomorphismus f: $i \mapsto a^i$ von letzter Folie
- f^{-1}: $a^i \mapsto i$, d.h. $f^{-1}(b) = i$ löst das DLP.

DLP in einigen Gruppen schwer:

- Berechnen von f in beide Richtungen nicht immer effizient.