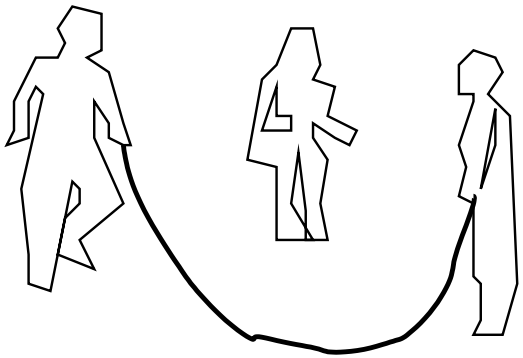
4: Gruppen



Definition 49

Sei G eine nichtleere Menge. Eine Funktion

$$\circ : G \times G \to G$$

bezeichnen wir als *Verknüpfung auf G*.
Das Paar $(G, \circ)$ bezeichnen wir als *Gruppoid*.

- Eine Funktion ist nur eine Verknüpfung wenn sie abgeschlossen ist, d.h. jede Ausgabe in G liegt
- Statt "$\circ(a, b)$" können wir auch "$a \circ b$" schreiben.
- Wenn klar ist, welche Verknüpfung $\circ$ wir meinen, schreiben wir auch "G" statt "$(G, \circ)$."
- Die *Ordnung* von G ist die Anzahl $|G|$ der Elemente in G.
- Wir nennen $(G, \circ)$ *kommutativ* (oder abelsch), wenn für alle $a, b \in G$ gilt

$$a \circ b = b \circ a.$$

Definition 50

- Gilt für alle a, b, c in dem Gruppoid $(G, \circ)$ die Beziehung

$$a \circ (b \circ c) = (a \circ b) \circ c,$$

dann heißt $\circ$ *assoziativ*, und $(G, \circ)$ ist eine **Halbgruppe**.

- Gibt es in der Halbgruppe G ein e, so dass für alle $a \in G$ gilt

$$e \circ a = a \circ e = a,$$

dann heißt e *neutrales Element*, und G ist ein **Monoid**.

- Gibt es in dem Monoid zu jedem $a \in G$ ein *Inverses* $\overline{a}$ in G mit

$$a \circ \overline{a} = e,$$

dann ist G eine **Gruppe**.

Eindeutigkeitssätze

Satz 51 (Eindeutigkeit des neutralen Elements)

In einer Halbgruppe gibt es höchstens ein neutrales Element.

Satz 52 (Eindeutigkeit der Inversen)

In einem Monoid gibt es zu jedem Element höchstens ein Inverses. Hat x ein Inverses x^{-1}, dann ist x selbst das Inverse von x^{-1}.

(Beweis: Übungsaufgabe)

Untergruppen

Definition 53

Sei $(G, \circ)$ eine Gruppe.
Wir nennen $(U, \circ)$ *Untergruppe* von $(G, \circ)$
(Schreibweise "$(U, \circ) \leq (G, \circ)$", bzw. "$U \leq G$"),
wenn gilt:

1. $U \subseteq G$ und
2. $(U, \circ)$ ist selbst eine Gruppe.

Ist e das neutrale Element von G, dann sind $\{e\}$ und G *triviale Untergruppen* von G. Alle anderen Untergruppen sind nichttrivial.

Untergruppen von Untergruppen

Satz 54 (Transitivität der Untergruppeneigenschaft)

Ist $(V, \circ) \leq (U, \circ) \leq (T, \circ)$ *eine Kette von Untergruppen, dann gilt auch* $(V, \circ) \leq (T, \circ)$.

Beweis.

Um nachzuweisen, dass $(V, \circ)$ eine Untergruppe von $(T, \circ)$ ist, müssen wir zwei Eigenschaften von V nachweisen:

1. $V \subseteq T$ und
2. $(V, \circ)$ ist eine Gruppe.

Die erste Eigenschaft folgt aus der Transitivität der Untermengeneigenschaft: $V \subseteq U \subseteq T \Rightarrow V \subseteq T$.
Weil $(V, \circ)$ eine Untergruppe von $(U, \circ)$ ist, ist $(V, \circ)$ insbesondere selbst eine Gruppe. Also gilt auch die zweite Eigenschaft. □

Nachweis der Untergruppen-Eigenschaft

Sei $(G, \circ)$ eine Gruppe mit neutralem Element e und $U \subseteq G$.

Wie können wir $(U, \circ) \leq (G, \circ)$ beweisen – oder ggf. widerlegen?
U muss die Eigenschaften einer Gruppe haben:

- *Assoziativität:* Weil $(G, \circ)$ eine Gruppe ist, ist für alle $a, b, c \in G$ die Gleichung
$$(a \circ b) \circ c = a \circ (b \circ c)$$
erfüllt, also erst recht für alle $a, b, c \in U \subseteq G$.
- *Kommutativität:* $(G, \circ)$ muss nicht kommutativ sein. Aber wenn $(G, \circ)$ kommutativ ist, dann ist $(U, \circ)$ erst recht kommutativ.
- Es gilt $(U, \circ) \leq (G, \circ)$ genau dann, wenn die folgenden drei Bedingungen erfüllt sind:
  1. *Abgeschlossenheit:* $\forall u, v \in U: u \circ v \in U$.
  2. *Neutrales Element:* $e \in U$.
  3. *Inverse Elemente:* $\forall u \in U: u^{-1} \in U$.

Beispiele (additiv)

- $(\mathbb{N}, -)$ und $(\mathbb{N}_0, -)$ sind keine Gruppoiden.
- $(\mathbb{Z}, -)$ ist ein Gruppoid, aber keine Halbgruppe.
- $(\mathbb{N}, +)$ ist eine Halbgruppe, aber kein Monoid.
- $(\mathbb{N}_0, +)$ ist ein Monoid mit neutr. El. 0, aber keine Gruppe.
- $(\mathbb{Z}, +)$ ist eine Gruppe mit neutr. El. 0.
- Sei $m\mathbb{Z} = \{a \in \mathbb{Z} : \exists k \in \mathbb{Z} : a = km\}$.
  Dann ist $(m\mathbb{Z}, +)$ eine Gruppe. (Beweis!)
- Es gilt $(m\mathbb{Z}, +) \leq (\mathbb{Z}, +)$.
  Ist $n|m$, dann ist $(m\mathbb{Z}, +) \leq (n\mathbb{Z}, +)$. (Beweis!)

Achtung: Mögliches Missverständnis!

$(\mathbb{Z}_n, +)$ ist eine Gruppe – aber keine Untergruppe von $(\mathbb{Z}, +)$.

Erklärung:

- $\mathbb{Z}_n$ ist "die Menge aller Restklassen modulo n".
- Die Restklasse von a mod n ist $\{kn + a | k \in \mathbb{Z}\} \subseteq \mathbb{Z}$.
- Eine Restklasse ist keine Zahl, sondern eine Menge von Zahlen!
- Trotz gleicher Schreibweise und gleichen Namens:
  Die Addition in $\mathbb{Z}$ und die Addition in $\mathbb{Z}_n$ sind verschiedene Operationen!

Isomorphie von Gruppen

Definition 55

Zwei Gruppen $(G, \circ)$ und $(H, \diamond)$ sind *isomorph* (zueinander), falls es eine Permutation $\pi : G \to H$ gibt, so dass $a, b \in G$ gilt:

$$\pi(a \circ b) = \pi(a) \diamond \pi(b).$$

In diesem Fall bezeichnen wir π als *Isomorphismus* von $(G, \circ)$ und $(H, \diamond)$.

Beispiel:

- Jede Gruppe ist isomorph zu sich selbst ($\pi(x) = x$).
- Die Gruppen $(\mathbb{Z}, +)$ und $(m\mathbb{Z}, +)$ sind isomorph.
  (Was ist der zugehörige Isomorphismus?)

Beispiele (multiplikativ)

- $(\mathbb{N}_0, *)$, $(\mathbb{N}, *)$ und $(\mathbb{Z}, *)$
  sind Monoide mit neutr. El. 1, aber keine Gruppen.
- $(\mathbb{Q}\backslash\{0\}, *)$ ist eine Gruppe mit neutr. El. 1.
- $(\mathbb{Z}_n, *)$ ist keine Gruppe. (Warum nicht?)
- Unter welchen Umständen ist $(\mathbb{Z}_n\backslash\{0\}, *)$ eine Gruppe?

4.1: Die Invertierbaren in einem Monoid

Sei $(G, \circ)$ ein Monoid mit neutralem Element e. Die *Menge der Invertierbaren Elemente in G* ist

$$G^* = \{ a \in G | \exists \overline{a} : a \circ \overline{a} = \overline{a} \circ a = e \}$$

Satz 56

1. $(G^*, \circ)$ *ist eine Gruppe.*
2. *Wenn* $(G, \circ)$ *kommutativ ist, dann ist auch* $(G^*, \circ)$ *kommutativ.*

(Wegen $G^* \subseteq G$ sind Assoziativität und, ggf., Kommutativität klar, und das neutrale Element $e \in G^*$.
Noch z.z.: Inverse Elemente, Abgeschlossenheit.)

Die Gruppe $(\mathbb{Z}_n^*, *)$

Sei $n \in \mathbb{N}$. Die Menge der Invertierbaren in $\mathbb{Z}_n$ ist

$$\mathbb{Z}_n^* = \left\{ z \in \mathbb{Z}_n | \exists \overline{z} \in G : z(z^{-1}) = (z^{-1})z = 1 \right\}.$$

Es gilt: $\mathbb{Z}_n^* = \{z \in \mathbb{Z}_n | \text{ggT}(z, n) = 1\}$. (Warum?)

Algebraische Eigenschaften von $\mathbb{Z}_n$ und $\mathbb{Z}_n^*$:

- $(\mathbb{Z}_n, +)$ ist eine Gruppe. (Wissen wir bereits.)
- $(\mathbb{Z}_n, *)$ ist keine Gruppe. (Wissen wir auch schon.)
- $(\mathbb{Z}_n^*, +)$ ist keine Gruppe. (Denn $0 \notin \mathbb{Z}_n^*$ wäre das neutr. El.)
- $(\mathbb{Z}_n^*, *)$ ist eine kommutative Gruppe. (Gerade bewiesen!)

Wie viele Elemente hat $\mathbb{Z}_n^*$?

Definition 57 (Eulersche φ-Funktion)

Sei $n \in \mathbb{N}$, dann ist $\varphi(n) = |\mathbb{Z}_n^*|$ die Ordnung von $\mathbb{Z}_n^*$.

Satz 58

1. *Sei p prim. Dann gilt $\varphi(p^r) = p^{r-1}(p-1)$ für $r \in \mathbb{N}$.*
   Insbesondere ist $\varphi(p) = p - 1$.
2. *Seien q_1 und q_2 teilerfremd. Dann gilt $\varphi(q_1 q_2) = \varphi(q_1)\varphi(q_2)$.*

Folgerung ($\rightarrow$ RSA)

Seien $p \neq q$ Primzahlen. Dann gilt $\varphi(p * q) = (p-1)(q-1)$.

4.2: Verknüpfungstafeln: Sudoku für Mathematiker

Ist $G = \{g_1 \ldots, g_n\}$ eine endliche Menge kann man eine Verknüpfung $\circ$ durch Angabe aller n^2 Werte $g_i \circ g_j$ festlegen.

Definition 59

Eine *Verknüpfungstafel* ist eine Tabelle, die für alle Elemente g_1, $\ldots$, g_n einer endlichen Gruppe G den Wert $g_i \circ g_j$ in Zeile i und Spalte j enthält.

$\circ$	g_1	$\cdots$	g_j	$\cdots$	g_n
g_1					
$\vdots$			$\vdots$		
g_i	$\cdots$		$g_i \circ g_j$		
$\vdots$					
g_n					

Eigenschaften von Verknüpfungstafeln

Satz 60

Ist $(G, \circ)$ eine endliche Gruppe, dann tritt in jeder Zeile und jeder Spalte der Verknüpfungstafel jeder Wert $g_i \in G$ genau einmal auf.

Satz 61

Eine endliche Halbgruppe ist genau dann kommutativ, wenn die zugehörige Verknüpfungstafel spiegelsymmetrisch bezüglich der Hauptdiagonalen (von links oben nach rechts unten) ist.

Beispiele

Für $(\mathbb{Z}_4, +)$:

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Für $(\mathbb{Z}_5 \setminus \{0\}, *)$:

$*$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Für $(\mathbb{Z}_4, \oplus)$:

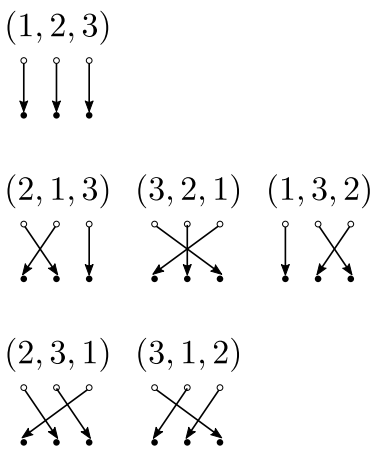
$\oplus$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

In $(\mathbb{Z}_4, \oplus)$ identifizieren wir Elemente $a \in \mathbb{Z}_4$ mit $(b, c) \in \mathbb{Z}_2^2$ und $\oplus$ mit der elementweisen Addition mod 2 ($\rightarrow$ Tafel).

Zwei dieser Gruppen sind isomorph zueinander, die dritte ist nicht isomorph zu den beiden anderen. (Welche und warum?)

4.3: Symmetrische Gruppen

- S_3 bezeichne die Menge der Permutationen über $\{1, 2, 3\}$.
- Man verwechsele S_3 nicht mit dem Definitions- und Wertebereich dieser Funktionen, denn $S_3 \neq \{1, 2, 3\}$!!!
- Tatsächlich enthält S_3 sechs Elemente:
  - Die "Identität" e: $(1, 2, 3)$
  - Drei Vertauschungen von genau zwei Elementen:
    $(2, 1, 3)$, $(3, 2, 1)$ und $(1, 3, 2)$
  - Zwei zyklische Vertauschungen aller drei Elemente:
    $(2, 3, 1)$ und $(3, 1, 2)$



(Man überzeuge sich, dass es keine anderen Permutationen über $\{1, 2, 3\}$ gibt.)

Eigenschaften von S_3

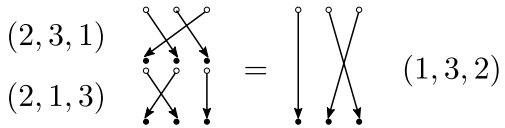
Verknüpfung: $(a \circ b)(x) = a(b(x))$ ("zuerst b anwenden, dann a").

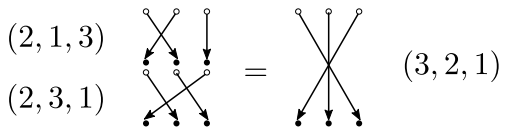
Gruppoid: Sind a und b Permutationen über $\{1, 2, 3\}$, dann ist auch $(a \circ b)$ eine solche.

Halbgruppe: $((a \circ b) \circ c)(x)$ und $(a \circ (b \circ c))(x)$ werden gleichermaßen zu $c(b(a(x)))$ aufgelöst.

S_3 ist nicht-kommutativ:

$$(2,1,3) \circ (2,3,1) \neq (2,3,1) \circ (2,1,3)$$





Monoid: Die Identität e ist das neutrale Element: $a \circ e = e \circ a = a$.

Ist S_3 eine Gruppe?

- Die Identität e ist selbstinvers: $e \circ e = e$.
- Vertauschungen von genau zwei Elementen sind selbstinvers:
  $(2,1,3) \circ (2,1,3) = e$, $(3,2,1) \circ (3,2,1) = e$ und
  $(1,3,2) \circ (1,3,2) = e$.
- Bleiben noch zwei Elemente, die nicht selbstinvers sind:
  $(2,3,1) \circ (2,3,1) = (3,1,2)$ und $(3,1,2) \circ (3,1,2) = (2,3,1)$
- Ist S_3 trotzdem eine Gruppe?
- **Ja!** Denn $(2,3,1) \circ (3,1,2) = (3,1,2) \circ (2,3,1) = e$!
- Allgemein:
  Die Identität ist eine Permutation, und
  das Inverse einer Permutation ist selbst eine Permutation.

Die Verknüpfungstafel von $(S_3, \circ)$

$\circ$	e	$(2,1,3)$	$(3,2,1)$	$(1,3,2)$	$(2,3,1)$	$(3,1,2)$
e	e	$(2,1,3)$	$(3,2,1)$	$(1,3,2)$	$(2,3,1)$	$(3,1,2)$
$(2,1,3)$	$(2,1,3)$	e	$(3,1,2)$	$(2,3,1)$	$(1,3,2)$	$(3,2,1)$
$(3,2,1)$	$(3,2,1)$	$(2,3,1)$	e	$(3,1,2)$	$(2,1,3)$	$(1,3,2)$
$(1,3,2)$	$(1,3,2)$	$(3,1,2)$	$(2,3,1)$	e	$(3,2,1)$	$(2,1,3)$
$(2,3,1)$	$(2,3,1)$	$(3,2,1)$	$(1,3,2)$	$(2,1,3)$	$(3,1,2)$	e
$(3,1,2)$	$(3,1,2)$	$(1,3,2)$	$(2,1,3)$	$(3,2,1)$	e	$(2,3,1)$

Die Symmetrischen Gruppen S_n

S_3 ist nur ein Beispiel aus einer großen Menge von Gruppen.

1. Für jedes $n \in \mathbb{N}$ ist die Symmetrische Gruppe S_n die Menge aller Permutationen über $\{1, \ldots, n\}$ mit dem Hintereinanderausführen als Verknüpfung.
2. Für jedes $n \in \mathbb{N}$ ist S_n tatsächlich eine Gruppe. (Warum?)
3. S_n ist eine Untergruppe von S_{n+1}. (Siehe nächste Folie!)
4. S_1 und S_2 sind kommutativ. (Warum?)
5. Für $n \geq 3$ ist S_n nicht kommutativ. (Warum nicht?)

Eigenschaften von S_n

Satz 62

Ist $i \geq 1$, $i \leq n$, dann ist S_i eine Untergruppe von S_n.

Beweis.

Es gilt $S_i \subseteq S_n$. Da S_i selbst eine Gruppe ist, folgt $S_i \leq S_n$.) □

Satz 63

Die Anzahl aller Permutationen über einer n-elementigen Menge, und damit die Anzahl aller Elemente von S_n ist

$$n! = n * (n-1) * (n-2) * \cdots * 2 * 1.$$

(Beweis durch Induktion nach n.)

4.4: Zyklische und endliche Gruppen

Definition 64

Sei $(G, \circ)$ eine Gruppe mit neutralem Element e.
Für $x \in G$ und $z \in \mathbb{Z}$ definieren wir

$$x^z = \begin{cases} x \circ (x^{z-1}) & \text{falls } z \geq 1, \\ e & \text{falls } z = 0 \text{ und} \\ 1/x^{-z} & \text{falls } z \leq -1. \end{cases}$$

Sei $x \in G$. Das kleinste $n \in \mathbb{N}$ mit $x^n = e$ bezeichnen wir als die *Ordnung* von x. Gibt es kein solches $n \in \mathbb{N}$, dann ist die Ordnung von x unendlich.

G heißt *zyklisch*, falls es ein $a \in G$ gibt mit $G = \{a^z | z \in \mathbb{Z}\}$.

Ein solches $a \in G$ nennen wir *Erzeuger* oder *Generator* von G.

Zyklische Gruppen, die wir bereits kennen

- $(\mathbb{Z}, +)$ ist zyklisch und von unendlicher Ordnung.
  Die einzigen Generatoren sind 1 und -1.
- $(\mathbb{Z}_n, +)$ ist zyklisch von der Ordnung $n \in \mathbb{N}$.
  (Was sind die Generatoren von $(\mathbb{Z}_n, +)$?)

Eigenschaften zyklischer Gruppen

Satz 65

1. *Alle zyklischen Gruppen sind kommutativ.*
2. *Ist die Gruppe G von endlicher Ordnung n,*
   dann ist die Ordnung eines jeden Elements ein Teiler von n.
3. *Ist G eine Gruppe und $x \in G$*
   dann ist $\langle x \rangle = \{x^z | z \in \mathbb{Z}\}$ eine Untergruppe von G.

Man kann sogar zeigen, dass alle zyklischen Gruppen isomorph zu einer der Gruppen $\mathbb{Z}$ bzw. $\mathbb{Z}_n$ sind.

Beispiel: Ist p prim, dann ist $(\mathbb{Z}_p \backslash \{0\}, *)$ eine zyklische Gruppe der Ordnung $p-1$, und damit isomorph zu $(\mathbb{Z}_{p-1}, +)$.

(Für $p = 5$ hatten wir diese Isomorphie schon beobachtet.)

Gruppen, die nicht zyklisch sind

1. Für $n \geq 3$ sind die Symmetrischen Gruppen S_n nicht zyklisch (sie sind ja nicht einmal kommutativ).
2. Wie wir noch sehen werden, haben sie jedoch zyklische Untergruppen ...
3. Die bereits bekannte Gruppe $(\mathbb{Z}_4, \oplus)$ ist zwar kommutativ, aber nicht zyklisch. Das neutrale Element hat die Ordnung 1, die Elemente 1, 2 und 3 haben Ordnung 2.

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

4. Aber: Alle $x \in \mathbb{Z}_4$ können wir durch die Verknüpfung von Elementen aus $\langle 1 \rangle$ und $\langle 2 \rangle$ generieren:
   $0 = 1^0 \oplus 2^0$, $1 = 1^1 \oplus 2^0$, $2 = 1^0 \oplus 2^1$, $3 = 1^1 \oplus 2^1$.

Das direkte Produkt von zwei Gruppen

Definition 66

Für zwei Gruppen $(G, \circ)$ und $(H, \diamond)$ ist das *direkte Produkt* $(G \times H, *)$ definiert durch die Grundmenge $G \times H$ und die Operation $* : (G \times H) \times (G \times H) \to G \times H$ mit

$$(a, b) * (c, d) = ((a \circ c), (b \diamond d)).$$

Satz 67

$(G \times H, *)$ ist eine Gruppe.

Wenn $e_G \in G$ und $e_H \in H$ die neutralen Elemente in G bzw. H sind, dann ist (e_G, e_H) das neutrale Element in $G \times H$.

$G \times \{e_H\}$ und $\{e_G\} \times H$ sind Untergruppen von $G \times H$.

(Beweis: Übungsaufgabe)

Beispiele

Man kann zeigen, dass

- S_3 isomorph ist zu $\langle (2,1,3) \rangle \times \langle (2,3,1) \rangle$ und
- $(\mathbb{Z}_4, \oplus)$ isomorph zu $\langle 1 \rangle \times \langle 2 \rangle$.

Allgemein kann man die endlichen kommutativen Gruppen wie folgt charakterisieren:

Satz 68

Jede endliche kommutative Gruppe ist entweder zyklisch, oder sie ist isomorph zum direkten Produkt von endlich vielen zyklischen Gruppen.

(Ohne Beweis.)

Untergruppen endlicher Gruppen

Satz 69 (Teilaussage des Satzes von Lagrange)

Sei G eine endliche abelsche Gruppe. Für jede Untergruppe U von G gilt: Die Ordnung von U ist ein Teiler der Ordnung von G.

(Ohne Beweis.)

Wir erinnern uns, dass bei der "effizienten" Berechnung von

$$4^{(4^4)} \bmod 13$$

etwas schiefgegangen war:

$$9 = 4^{(4^4)} \bmod 13 \neq 4^{(4^4) \bmod 13} \bmod 13 = 4^9 \bmod 13 = 12.$$

Der Satz von Lagrange liefert die Erklärung, was schiefgegangen ist ... und wie man es besser macht.

Das 444-Problem (noch einmal)

Gesucht:

$$4^{(4^4)} \pmod{13}.$$

Beobachtungen:

1. Z_{13}^* ist eine Gruppe der Ordnung 12.
2. Nach dem Satz von Lagrange haben alle Untergruppen von Z_{13}^* eine Ordnung, die ein Teiler von 12 ist – insbesondere auch die von 4 erzeugte Untergruppe.
3. Also können wir im Exponenten mod 12 rechnen! **Ah!**

Verallgemeinerung:

Satz 70 (Euler)

Für alle $a, b, m \in \mathbb{N}$, mit $ggT(a, m) = 1$ gilt:

$$a^b \bmod m = a^{b \bmod \varphi(m)} \bmod m.$$

Das 444-Problem (Effizienteste Lösung)

Gesucht:

$$4^{(4^4)} \pmod{13}.$$

Beobachtet:

$$\varphi(13) = 12.$$

Rechnung im Exponenten:

$$4^4 = 2^8 = 256 \quad \text{und} \quad 256 \bmod 12 = 4.$$

Also ist

$$4^{(4^4)} \bmod 13 = 4^4 \bmod 13.$$

Damit erhalten wir sehr effizient:

$$4^{(4^4)} \bmod 13 = (4 * (4 * (4 * 4) \bmod 13) \bmod 13) \bmod 13 = 9 \bmod 13.$$

4.5: Anwendung: Der Diffie-Hellman Schlüsselaustausch

Vorbereitung:

1. Wähle eine “große” Primzahl p, so dass
2. die Faktorisierung von $p-1$ bekannt ist.
3. Wähle eine “hinreichend große” Primzahl $q|(p-1)$ und ein Element $g \in (\mathbb{Z}_p^*, *)$ der Ordnung q.
4. Arithmetik mod p – aber tatsächlich werden wir in der Untergruppe $\langle g \rangle$ von $(\mathbb{Z}_p^*, *)$ rechnen.

Alice und Bob vereinbaren einen gemeinsamen geheimen Schlüssel

1. Alice wählt $\mathbf{a} \in \mathbb{Z}_q$ und veröffentlicht $\mathbf{A} := g^{\mathbf{a}} \pmod{p}$
   $(*$ **a** ist geheim $*)$
2. Bob wählt $\mathbf{b} \in \mathbb{Z}_q$ und berechnet $\mathbf{B} := g^{\mathbf{b}} \pmod{p}$
   $(*$ **b** ist geheim $*)$
3. Gemeinsamer geheimer Schlüssel von Alice und Bob:

$$\mathbf{B}^{\mathbf{a}} = g^{\mathbf{ab}} = \mathbf{A}^{\mathbf{b}}.$$

Beispiel (in winzigen Zahlen)

0. $p = 11$, $g = 4$,
   es ist $4^5 \equiv 1024 \equiv 1 \pmod{11}$, also $q = 5$.
1. $\mathbf{a} = 4$, $\mathbf{A} = 4^{\mathbf{4}} \equiv 3 \pmod{11}$.
2. $\mathbf{b} = 3$, $\mathbf{B} = 4^{\mathbf{3}} \equiv 9 \pmod{11}$.
3. Die Berechnung des geheimen Schlüssels:

$$\begin{aligned} \mathbf{B}^{\mathbf{a}} = 6561 &\equiv 5 \pmod{11}, \\ \mathbf{A}^{\mathbf{b}} = 27 &\equiv 5 \pmod{11}, \\ g^{\mathbf{ab}} = 16777216 &\equiv 5 \pmod{11}. \end{aligned}$$

Alice und Bob haben sich auf 5 als Geheimnis geeinigt.
Ein Angreifer müsste $g^{\mathbf{ab}} = 5$ berechnen, obwohl er weder $\mathbf{a}$ noch $\mathbf{b}$ kennt.

Ist der D.-H. Schlüsselaustausch sicher?

Man betrachte die folgenden beiden Probleme:

- Diskreter Logarithmus: Geg. $\mathbf{X} = g^{\mathbf{x}}$, berechne $\mathbf{x}$
- Diffie-Hellman-Problem: Gegeben $\mathbf{A}$ und $\mathbf{B}$, berechne $g^{\mathbf{ab}}$.
- Man beachte: Wenn man effizient Diskrete Logarithmen berechnen kann, dann kann man erst recht das Diffie-Hellman Problem effizient lösen.
- Ist das Diffie-Hellman Problem dagegen nicht effizient lösbar, dann kann ein Angreifer, der nur $\mathbf{A}$ und $\mathbf{B}$ kennt, den geheimen Schlüssel $g^{\mathbf{ab}}$ nicht berechnen.

Für Sicherheit gegen (bekannte) Algorithmen zur Berechnung des Diskreten Logarithmus wird empfohlen:

- p ist mindestens eine 2000-bit Primzahl und
- die Ordnung q von g ist mindestens eine 160-bit Primzahl.

Ist die Arithmetik mod p wirklich nötig?

Tatsächlich können wir, statt in $\langle g \rangle \leq \mathbb{Z}_p^*$ in **jeder beliebigen Gruppe** $(G, *)$ rechnen, die die folgenden drei *funktionalen Bedingungen* erfüllt:

1. die Ordnung q von G ist bekannt
   (um zufällige Zahlen $\mathbf{a}, \mathbf{b} \in \{0, \ldots, q-1\}$ zu wählen),
2. man kann in G effizient rechnen
   (um $g^{\mathbf{a}}$, $g^{\mathbf{b}}$, $\mathbf{B}^{\mathbf{a}}$ und $\mathbf{A}^{\mathbf{b}}$ zu berechnen)
3. und Gruppenelemente in G sind eindeutig darstellbar
   (damit $\mathbf{B}^{\mathbf{a}}$ und $\mathbf{A}^{\mathbf{b}}$ tatsächlich die gleiche Folge von Bits darstellen – statt verschiedener Repräsentationen des gleichen Elements von G).

Die Gruppe $(G, *) = (\mathbb{Z}_q, +)$ erfüllt alle drei Bedingungen.

Warum rechnen wir dann nicht einfach in $(\mathbb{Z}_q, +)$?

Zusätzlich zu den funktionalen Eigenschaften muss die Gruppe $(G, *)$ aber auch eine *Sicherheitsbedingung* erfüllen:

4. Man darf das Diffie-Hellman-Problem in $(G, *)$ nicht effizient lösen können.

   Insbesondere darf es in $(G, *)$ nicht effizient möglich sein, Diskrete Logarithmen zu berechnen.

Die Gruppe $(G, *) = (\mathbb{Z}_q, +)$, erfüllt diese Bedingung leider nicht.
(Warum nicht?)
(Wie kann man "Diskrete Logarithmen" in $(\mathbb{Z}_q, +)$ berechnen?)

Alternativen zur modularen Arithmetik?

Kryptographen suchen seit langem nach Alternativen zur Arithmetik mod p. Viele Gruppen $(G, *)$ wurden untersucht und als praxisuntauglich verworfen.

Insbesondere: Ist "$*$" effizient berechenbar und q "klein" (z.B. $q < 2^{140}$), dann kann man Diskrete Logarithmen in $(G, *)$ effizient berechnen ($\rightarrow$ Diskrete Wahrscheinlichkeit).

Eine Alternative, die in der Praxis allmählich an Bedeutung gewinnt, sind die *Punktgruppen Elliptischer Kurven*. Ihr besonderer Vorteil ist, dass sie die Verwendung kürzerer öffentlicher Schlüssel erlauben. Weitere Informationen:

`http://de.wikipedia.org/wiki/Elliptic_Curve_Cryptography`

4.6: Abstraktes mathematisches Denken

Statt nach spezifischen Lösungen für einzelne Probleme sucht man in Informatik und Ingenieurwissenschaften nach Algorithmen, die man möglichst vielfältig nutzen bzw. wiederverwerten kann. Das erfordert *eine bestimmte Form des abstrakten mathematischen Denkens:*

- **Welche grundlegenden Eigenschaften meiner vorhandenen Datenstrukturen reichen aus,**
  damit ein Algorithmus das leistet, was er leisten soll?
- **Gibt es andere Datenstrukturen, die diese Eigenschaften auch erfüllen?**

Um entsprechend abstrakte und allgemein nutzbare Algorithmen auch allgemein und abstrakt implementieren zu können, unterstützen fast alle modernen Programmiersprachen die objektorientierte und/oder die generische Programmierung.