Grundlagen

1. Recap Gruppen (insbes. $\mathbb{Z}_n^*$)
2. Eulersche φ-Funktion
3. verschiedene Gesetzmässigkeiten bezüglich Gruppen
4. zyklische Gruppen
5. RSA

Recap: Gruppe

$(G, *)$ heisst Gruppe, wenn die folgenden Bedingungen erfüllt sind:

- **Assozitativität:** $(a * b) * c = a * (b * c)$ für alle $a, b, c \in G$
- **Neutralelement:** Es existiert ein Element $e \in G$ mit $e * a = a$ für alle $a \in G$
- **Inverses:** Für jedes $a \in G$ existiert ein Inverses a^{-1} mit der Eigenschaft: $a * a^{-1} = e$
- **Abgeschlossenheit:** $a * b \in G$ für alle $a, b \in G$

Beispiele:

- $\mathbb{Q}^* := \mathbb{Q} \backslash \{0\}$ mit Multiplikation
- $\mathbb{Z}$ mit Addition
- $\mathbb{Z}_n^*$ (s. nächste Folie)

Bem: Im Exponent kann auch eine negative ganze Zahl stehen.

- Bsp: a^{-3} steht für $a^{-1} \cdot a^{-1} \cdot a^{-1}$
  (In $\mathbb{Z}_{11}^*$ ist $2^{-1} = 6$ und $2^{-3} = \left(2^{-1}\right)^3 = 6^3 = 7 \pmod{11}$.)

Recap: $\mathbb{Z}_n^*$

Definition der Gruppe $\mathbb{Z}_n^*$

- Die Elemente sind alle zu n teilerfremden Zahlen in $\{1, 2, \ldots, n-1\}$
- Die Gruppen-Operation entspricht der Multiplikation

- **Bsp** $\mathbb{Z}_{12}^* = \{1, 5, 7, 11\}$
- **Zum Aufwärmen:** $\mathbb{Z}_{14}^*$ = ?
  In $\mathbb{Z}_{14}^*$:
  - 11^{-1} = ?
  - 5^{-4} = ?

Eulersche φ-Funktion

- **Def:** $\varphi(n) := |\mathbb{Z}_n^*|$

Gesetzmässigkeiten (ohne Herleitungen)

(1) $\varphi(u \cdot v) = \varphi(u) \cdot \varphi(v)$, falls $\mathrm{ggT}(u, v) = 1$
(2) $\varphi(p) = p - 1$, falls p eine Primzahl ist
(3) $\varphi(p^k) = p^k - p^{k-1}$, falls p eine Primzahl ist

Aufwärm-Übung

- $|\mathbb{Z}_{15}^*|$ = ?
- $|\mathbb{Z}_{231}^*|$ = ?

Recap: Untergruppen

Definition Untergruppe

U ist eine **Untergruppe** von G, wenn

- es sich um eine Teilmenge handelt, und
- U selber eine Gruppe bildet.

Satz von Lagrange (ohne Herleitung)

Ist U eine Untergruppe von G, so gilt: $|U|$ teilt $|G|$.

Definition erzeugte Untergruppe

Für jedes Element $g \in G$ heisst $< g > := \{1, g, g^2, g^3, \ldots\}$ die von g **erzeugte Untergruppe**

Folgerungen

- $| < g > | = \min\{k : g^k = 1\}$
- $| < g > |$ teilt $|G|$
- $g^{|G|} = 1$

Ordnung eines Elements einer Gruppe

Definition

Die Ordnung eines Elementes g bezeichnet $| < g > |$.

Beispiele: Wir betrachten nochmals $\mathbb{Z}_{14}^{*} = \{1, 3, 5, 9, 11, 13\}$.

- Ordnung vom Element 9?
- Ordnung vom Element 3?
- Ordnung vom Element 13?

Folgerungen aus der Gleichung $g^{|G|} = 1$

Satz von Euler

$a^{\varphi(n)} = 1 \pmod{n}$ für alle $a \in \mathbb{Z}_n^*$

Für den Spezialfall, dass n eine Primzahl ist:

Kleiner Satz von Fermat

Für jede Primzahl p gilt:

$$a^{p-1} = 1 \pmod{p}, \text{ für alle } a \in \mathbb{Z}_p^*$$

Zyklische Gruppen

Definition

Eine Gruppe G heisst **zyklisch**, falls es ein $g \in G$ gibt mit der Eigenschaft

$$G = \{1, g, g^2, g^3, \ldots\}$$

g heisst **Erzeugendes** oder **Primitivwurzel**

Beispiel: In $\mathbb{Z}_7^*$ ist $< 5 >= \{5, 4, 6, 2, 3, 1\} = \mathbb{Z}_7^*$. Somit

- 5 ist Erzeugendes von $\mathbb{Z}_7^*$, und
- $\mathbb{Z}_7^*$ ist zyklisch.

Aufgabe: Verifiziere, dass $\mathbb{Z}_{11}^*$ zyklisch ist.

Satz (ohne Herleitung)

Für jede Primzahl p gilt: $\mathbb{Z}_p^*$ ist zyklisch.

Effiziente Bestimmung der Ordnung eines Elementes

Beispiel: Gesucht ist die Ordnung vom Element 3 in $\mathbb{Z}_{83}^*$.
Fragestellung: Wie lässt sich die Ordnung mit **möglichst wenigen** Operationen bestimmen?

- Naiver Ansatz: Berechnung von $\{3, 3^2, 3^3, \ldots\}$: zeitraubend!
- Überlegung: Welche Werte kommen überhaupt in Frage?

Einsatz der obigen Idee für weitere Beispiele

- Ordnung von 5 in $\mathbb{Z}_{83}^*$?
- Ordnung von 7 in $\mathbb{Z}_{23}^*$?

Folgerung für Erzeugende

Recap: Ein Element g ist ein Erzeugendes von G, wenn seine Ordnung gleich $|G|$ ist.

Satz (Kriterium für Erzeugende)

Für jedes Element g einer Gruppe G mit $n := |G|$ gilt:
Falls $g^{\frac{n}{p}} \neq 1$ für **jeden** Primteiler p von n, so ist g ein Erzeugendes.

Aufgabe: Entscheiden Sie, ob $a = 2$ eine Primitivwurzel in $\mathbb{Z}_{37}^*$ ist.

Recap: Ringe und Körper

- Erinnerung: Das **Distributivgesetz** ist erfüllt, wenn für alle a, b, c gilt: $a \cdot (b + c) = a \cdot b + a \cdot c$ resp. $(a + b) \cdot c = a \cdot c + b \cdot c$

Definition Ring

Eine Menge R mit den Operationen "+" und "·" heisst **Ring**, wenn

- R bezüglich Addition eine abelsche Gruppe bildet, und
- Die Multiplikation assoziativ ist, d.h. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
- Das Distributivgesetz ist erfüllt.

Definition Körper

Eine Menge K mit den Operationen "+" und "·" heisst **Körper**, wenn

- K bezüglich Addition eine abelsche Gruppe bildet, und
- $K \backslash \{0\}$ bezüglich Multiplikatione eine abelsche Gruppe bildet
- Das Distributivgesetz ist erfüllt.

- **Beispiel für einen Körper:** $\mathbb{Z}_p$ für eine Primzahl p

Recap: RSA

- öffentlicher Schlüssel: (e, N)
- privater Schlüssel: d
- Eigenschaften:
  - N ist das Produkt zweier Primzahlen
  - $e \cdot d = 1 \pmod{\varphi(N)}$
- Verschlüsselung einer Nachricht m: $c := m^e \pmod{N}$
- Entschlüsselung eines Chiffrates: $m := c^d \pmod{N}$
- **Beispiele:** s. Übungen
- **Bem:** Die Sicherheit von RSA beruht darauf, dass eine grosse Zahl N schwierig zu faktorisieren ist (nach heutigem Wissens-Stand).