Satz von Euler

Satz von Euler

Sei $(G, \cdot)$ eine endl. abelsche Gruppe. Dann gilt $a^{|G|} = 1$ für alle $a \in G$.

Beweis:

- Sei $G = \{g_1, \ldots, g_n\}$ und $a \in G$. Betrachte die Abbildung
$$f : G \to G, g \mapsto ag.$$
- Da $a \in G$, besitzt a ein Inverses. D.h. f ist eine Bijektion auf G.
- Damit gilt $\{g_1, \ldots, g_n\} = \{f(g_1), \ldots, f(g_n)\} = \{ag_1, \ldots, ag_n\}$.
- Es folgt $\prod_{i=1}^n g_i = \prod_{i=1}^n ag_i = a^n \prod_{i=1}^n g_i$.
- Kürzen von $\prod_{i=1}^n g_i$ liefert $a^n = a^{|G|} = 1$.

Korollar 1

Sei $n \in \mathbb{N}$. Für alle $\bar{a} \in U_n$ gilt $\bar{a}^{|U_n|} = \bar{a}^{\varphi(n)} = \bar{1}$.

Korollar 2 Kleiner Fermat

Sei $p \in \mathbb{P}$. Für alle $\bar{a} \in U_p$ gilt $\bar{a}^{|U_p|} = \bar{a}^{p-1} = \bar{1}$.

Satz von Lagrange

Definition Gruppen-Notation

Sei $(G, \cdot)$ eine endliche abelsche Gruppe. Sei $a \in G$. Wir definieren

1. $\mathrm{ord}(a) = \min\{i \in \mathbb{N} \mid a^i = 1\}$ ist die *Ordnung von a*.
2. $H \subseteq G$ ist *Untergruppe* von G, falls $(H, \cdot)$ eine Gruppe ist.
3. $\langle a \rangle = \{a, a^2, \ldots, a^{\mathrm{ord}(g)}\}$ ist die von a erzeugte Untergruppe.

Bsp: In U_7 gilt $\langle \bar{2} \rangle = \{\bar{2}, \bar{4}, \bar{1}\}$.

Satz von Lagrange

Sei $(G, \cdot)$ eine endl. abelsche Gruppe. Für alle $a \in G$ gilt $\mathrm{ord}(a) \mid |G|$.

Beweis:

- Annahme: $\mathrm{ord}(a) \nmid |G|$. Dann liefert Euklidische Division
$$|G| = q \cdot \mathrm{ord}(a) + r \text{ mit } 0 < r < \mathrm{ord}(a).$$
- Nach Satz von Euler gilt
$$1 = a^{|G|} = a^{q \cdot \mathrm{ord}(a) + r} = (a^{\mathrm{ord}(a)})^q \cdot a^r = 1^q \cdot a^r = a^r.$$
- D.h. $a^r = 1$, $r < \mathrm{ord}(a)$. (Widerspruch zur Minimalität von $\mathrm{ord}(a)$)

Diffie-Hellman Schlüsselaustausch

Ziel:

Austausch eines *geheimen* Schlüssels über einen *öffentlichen* Kanal.
Definiere die Funktion $\exp_{\bar{g}} : \mathbb{Z}/(p-1)\mathbb{Z} \to U_p,\ \bar{a} \mapsto \bar{g}^{\bar{a}} = \bar{g}^a$

Protokoll Diffie-Hellman Schlüsselaustausch (1976)

öffentliche Parameter: $p \in \mathbb{P}$ und $\bar{g} \in U_p$ mit $\langle \bar{g} \rangle = U_p$

1. Alice wählt $a \in \mathbb{Z}/(p-1)\mathbb{Z}$ und sendet $\exp_{\bar{g}}(a) = \bar{g}^a$ an Bob.
2. Bob wählt $b \in \mathbb{Z}/(p-1)\mathbb{Z}$ und sendet $\exp_{\bar{g}}(b) = \bar{g}^b$ an Alice.
3. Alice berechnet $\exp_{\bar{g}^b}(a) = \bar{g}^{ab}$, Bob berechnet $\exp_{\bar{g}^a}(b) = \bar{g}^{ab}$.

gemeinsamer Schlüssel: $\bar{g}^{ab}$

Sicherheit:

- Ein Angreifer muss aus $p, \bar{g}, \bar{g}^a, \bar{g}^b$ den Wert $\bar{g}^{ab}$ berechnen.
- Dies kann auf das *Diskrete Logarithmus Problem* zurückgeführt werden: Berechne a aus $p, \bar{g}, \bar{g}^a$.
- *Vermutung:* $\exp_g(\cdot)$ ist eine sogenannte *Einwegfunktion*, d.h. leicht zu berechnen, aber schwer zu invertieren.

Das RSA-Kryptosystem

Ziel: Public-Key Kryptographie, d.h. Verschlüsselung ohne vorherigen Austausch eines geheimen Schlüssels.

Protokoll RSA Public Key Verschlüsselung (1977)

1. **Schlüsselgenerierung** von Alice: Wähle $p, q \in \mathbb{P}$ und berechne $N = pq$ und $\varphi(N)$. Wähle $e \in U_{\varphi(N)}$. Berechne $d \in U_{\varphi(N)}$ mit $ed \equiv 1 \bmod \varphi(N)$. Veröffentliche (N, e), d bleibt geheim.
2. **Verschlüsselung** von Bob: Für ein $\bar{m} \in \mathbb{Z}/N\mathbb{Z}$ berechne
$$\mathrm{Enc}_{N,e} : \mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/N\mathbb{Z},\ \bar{m} \mapsto \bar{m}^e.$$
3. **Entschlüsselung** durch Alice: Für ein $\bar{c} = \bar{m}^e \in \mathbb{Z}/N\mathbb{Z}$ berechne
$$\mathrm{Dec}_{N,d} : \mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/N\mathbb{Z},\ \bar{c} \mapsto \bar{c}^d.$$

Korrektheit:

- Nach Satz von Euler gilt für alle $\bar{m} \in U_N$
$$\mathrm{Dec}_{N,d}(\mathrm{Enc}_{N,e}(\bar{m})) = (\bar{m}^e)^d = \bar{m}^{1+k\varphi(N)} = \bar{m} \cdot (\bar{m}^{\varphi(N)})^k = \bar{m}.$$
- **Übung:** Zeigen Sie die Korrektheit für $\bar{m} \in (\mathbb{Z}/N\mathbb{Z}) \setminus U_N$.

Sicherheit von RSA

Sicherheit von RSA:

- Kann man $N = pq$ faktorisieren, so kann man entschlüsseln.
- Berechnung von $\varphi(N)$ ist so schwer wie die Faktorisierung von N.
- Sei $\varphi(N) = (p-1)(q-1) = N - p - q + 1$ bekannt.
- Dann sind auch die Koeffizienten folgenden Polynoms bekannt
$$(x-p)(x-q) = x^2 - (p+q)x + N.$$
- Dessen Nullstellen p, q können effizient bestimmt werden (z.B. mittels Newton-Iteration).
- Damit erhält man die Faktorisierung von N.
- Das Berechnen von d ist so schwer wie Faktorisieren (nicht trivial).
- **Offenes Problem:**
Ist das Invertieren von $\bar{m} \mapsto \bar{m}^e$ so schwer wie Faktorisieren?

Endliche Körper

Satz Endliche Körper

Sei $p \in \mathbb{N}$. $\mathbb{Z}/p\mathbb{Z}$ ist ein Körper gdw $p \in \mathbb{P}$.

Beweis:

- $(\mathbb{Z}/p\mathbb{Z}, +)$ ist eine abelsche Gruppe. Kommutativität der Multiplikation und Distributivität vererben sich von $\mathbb{Z}$ auf $\mathbb{Z}/p\mathbb{Z}$.

$\Leftarrow$: Sei p prim. Dann gilt $\mathrm{ggT}(a, p)$ für alle $a \in \mathbb{Z}$ mit $p \nmid a$.

- Damit ist $U_p = \mathbb{Z}/p\mathbb{Z} \setminus \{\bar{0}\}$, d.h. $(\mathbb{Z}/p\mathbb{Z} \setminus \{\bar{0}\}, \cdot)$ ist eine Gruppe.

$\Rightarrow$: Sei $p = a \cdot b$ mit $1 < a, b < p$.

- Dann ist $(\mathbb{Z}/p\mathbb{Z} \setminus \{\bar{0}\}, \cdot)$ nicht abgeschlossen, da
$$\bar{a} \cdot \bar{b} = \bar{p} = \bar{0}, \text{ aber } \bar{a}, \bar{b} \neq \bar{0}.$$
- Damit ist $(\mathbb{Z}/p\mathbb{Z} \setminus \{\bar{0}\}, \cdot)$ keine Gruppe.

Endliche Körper $\mathbb{F}_p$

Definition Endliche Körper

Sei $p \in \mathbb{P}$. Wir bezeichnen den endlichen Körper $\mathbb{Z}/p\mathbb{Z}$ mit

$$\mathbb{F}_p \text{ bzw. } GF(p).$$

Bsp:

- In $\mathbb{F}_5$ gilt $\frac{\bar{3}}{\bar{2}} + \bar{1} = \bar{3} \cdot \overline{2^{-1}} + \bar{1} = \bar{3} \cdot \bar{3} + \bar{1} = \bar{0}$.
- In $\mathbb{F}_7$ gilt $\frac{\bar{3}}{\bar{2}} + \bar{1} = \bar{3} \cdot \overline{2^{-1}} + \bar{1} = \bar{3} \cdot \bar{4} + \bar{1} = \overline{-1}$.

Mehr endliche Körper

Ziel: Konstruktion von Körpern mit p^r Elementen für $r \geq 2$.

- Wir betrachten den Polynomring $\mathbb{F}_p[X]$ mit Koeffizienten aus $\mathbb{F}_p$.
- Aus den Übungen wissen wir, dass $\mathbb{F}_p[X]$ euklidisch ist mit der Gradfunktion $\deg(\cdot)$ als Bewertungsfunktion.
- Damit ist $\mathbb{F}_p[X]$ ein Hauptidealring und faktoriell.
- Für die Einheiten von $\mathbb{F}_p[X]$ gilt
$$(\mathbb{F}_p[X])^* = \{f \in \mathbb{F}_p[X] \mid \deg(f) = 0\}.$$
- Ein $f \in \mathbb{F}_p[X]$ heißt damit irreduzibel (bzw. prim), falls
$$f = rs \Rightarrow \deg(r) = 0 \text{ oder } \deg(s) = 0.$$

Mehr endliche Körper

- Setze $R_p := \mathbb{F}_p[X]$. Für $f, g, h \in \mathbb{F}_p[X]$ definieren wir
$$f \equiv g \bmod h \Leftrightarrow h | f - g.$$
- Die Äquivalenzklassen dieser Relation besitzen die Form
$$\bar{f} = f + R_p h = \{f + k \cdot h \mid k \in R_p\}.$$
- Die Menge aller Restklassen bezeichnen wir mit
$$R_p/h = \mathbb{F}_p[X]/h = \{f + k \cdot q \mid f \in \mathbb{F}_p[X]\}.$$
- Sei $\deg(q) = r$. Ein vollst. Repräsentantensystem für $\mathbb{F}_p[X]/h$ ist
$$R = \{f_0 + f_1 X + \dots f_{r-1} X^{r-1} \in \mathbb{Z}[X] \mid f_i \in \{0, \dots, p-1\}.\}$$
- Insbesondere gilt $|\mathbb{F}_p[X]/h| = |R| = p^r$.
- Ferner ist $\mathbb{F}_p[X]/h$ ein Körper gdw h irreduzibel ist über $\mathbb{F}_p$.
- Da für jedes p, r ein über $\mathbb{F}_p$ irreduzibles h mit $\deg(h) = r$ existiert, existiert stets ein Körper F_{p^r} mit p^r Elementen.

- **Warnung:** $\mathbb{F}_{p^r}$ ist nicht isomorph zu $\mathbb{Z}/p^r\mathbb{Z}$ (letzterer ist kein Körper).