4. Die prime Restklassengruppe und Anwendungen

4.1 Die prime Restklassengruppe

4.1.1 Satz

Sei R ein endlicher Ring, R_N die Menge der Nullteiler, dann ist

$$R = R^* \dot{\cup} R_N.$$

Beweis:

„$\supseteq$" klar.

„$\subseteq$" Sei $x \in R$, $x \notin R_N$.

Betrachte $\varphi: R \longrightarrow R: y \longmapsto x \cdot y$

Beh: φ ist injektiv.

Sei $\varphi(y_1) = \varphi(y_2) \Rightarrow x \cdot y_1 = x \cdot y_2$

$\Rightarrow x \cdot (y_1 - y_2) = 0 \overset{x \notin R_N}{\Rightarrow}$

$y_1 - y_2 = 0 \Rightarrow y_1 = y_2$

Da R endlich folgt, daß φ auch surjektiv ist.

Für $1 \in R$ $\exists$ Urbild $y \in R$:

$\varphi(y) = 1 = x \cdot y \Rightarrow x \in R^*$. □

Bsp $\mathbb{Z}_6^* = \{1,5\}$, $(\mathbb{Z}_6)_N = \{0,2,3,4\}$

Bem: $\bar{a} \in \mathbb{Z}_n$ ist Einheit $\Leftrightarrow$
$\exists b: \bar{a}\bar{b} = \bar{1} \in \mathbb{Z}_n \Leftrightarrow \exists k:$
$ab - 1 = k \cdot n \overset{\text{Bézout (1.7)}}{\Leftrightarrow} ggT(a,n) = 1$

4.1.2 Def $\mathbb{Z}_n^* = \{\bar{a} \mid ggT(a,n) = 1\}$
heißt die prime Restklassengruppe,
ihre Elemente prime Restklassen.

4.1.3 Korollar
Sei $n = p_1^{r_1} \cdots p_k^{r_k} \in \mathbb{Z}$ die Zerlegung in Primfaktoren, so ist
$\mathbb{Z}_n^* \cong \mathbb{Z}_{p_1^{r_1}}^* \times \cdots \times \mathbb{Z}_{p_k^{r_k}}^*$
Beweis mit dem chinesischen Restsatz 3.7.3.

4.1.4 Def $\varphi: \mathbb{N} \to \mathbb{Z}$,

$\varphi(n) := \#\{ r \in \mathbb{Z} \mid 1 \leq r \leq n, \ ggT(r,n) = 1 \}$

$= |\mathbb{Z}_n^*|$ = Ordnung der primen Restklassengruppe

heißt Eulersche φ-Funktion.

4.1.5 Satz (Fermat-Euler)

Seien $a, n \in \mathbb{Z}$, $n \geq 1$, $ggT(a,n) = 1$.

Dann gilt $a^{\varphi(n)} \equiv 1 \mod n$

Beweis: $a \in \mathbb{Z}_n^*$, $\varphi(n) = |\mathbb{Z}_n^*|$, die Ordnung von a teilt die Gruppenordnung (2.3.9, Korollar von Lagrange) $\Rightarrow$ $\overline{a}^{\varphi(n)} = \overline{1}$. □

4.1.6 Korollar

Sei p prim, $p \nmid a$

$\Rightarrow a^{p-1} \equiv 1 \mod p$

Beweis: $\varphi(p) = p-1$ □

4.1.7 Satz (Kleiner Satz von Fermat)

Sei p eine Primzahl, $a \in \mathbb{Z}$

$\Rightarrow \quad a^p \equiv a \mod p$

Beweis: Falls $p \mid a$ ist $a^p \equiv 0 \equiv a$.

Falls $p \nmid a$ ist $a^{p-1} \equiv 1 \Rightarrow$

$a^p \equiv a$. $\square$

4.1.8 Satz

Sei $n = p_1^{r_1} \cdots p_k^{r_k} \in \mathbb{Z}$ die Zerlegung in Primfaktoren.

Dann ist $\varphi(n) = \prod_{i=1}^{k} \varphi(p_i^{r_i})$

$$= \prod_{i=1}^{k} p_i^{r_i - 1}(p_i - 1)$$

Beweis:

$\varphi(p^r) = \#\{a \mid 1 \leq a \leq p^r, \ ggT(a, p^r) = 1\}$

$= p^r - \#\{\text{Vielfache von } p \text{ zwischen } 1 \text{ und } p^r\}$

$= p^r - p^{r-1} = p^{r-1}(p-1)$.

Damit folgt die zweite Gleichheit, die erste folgt aus dem chinesischen

Restsatz 3.7.3 bzw. 4.3. □

4.1.9 Korollar

Sei $G = \langle g \rangle$ eine zyklische Gruppe. Sei $|G| = n$, $d \mid n$. Dann gibt es $\varphi(d)$ Elemente der Ordnung d in G, $\{g^{r \cdot \frac{n}{d}} \mid 1 \leq r \leq d, ggT(r,d) = 1\}$.

Insbesondere gibt es $\varphi(n)$ Elemente der Ordnung n, also Erzeuger.

Folgt aus dem Satz über Untergruppen zyklischer Gruppen, 2.3.13 (4).

Bsp.

$(\mathbb{Z}_{12}, +)$

Element	0	1	2	3	4	5	6	7	8	9	10	11
Ordnung	1	12	6	4	3	12	2	12	3	4	6	12

$\varphi(12) = \varphi(4) \cdot \varphi(3) = 2(2-1) \cdot (3-1) = 4$

Erzeuger von $\mathbb{Z}_{12}$: 1, 5, 7, 11

$\varphi(6) = \varphi(2) \cdot \varphi(3) = 2$,

Elemente der Ordnung 6:

$\left(1 \cdot \frac{12}{6}\right) \cdot 1 = 2, \left(5 \cdot \frac{12}{6}\right) \cdot 1 = 10$,

denn $\{1,5\} = \{r \mid 1 \leq r \leq 6, ggT(r,6)=1\}$

$\varphi(2) = 1$, Element der Ordnung 2:

$\left(1 \cdot \frac{12}{2}\right) \cdot 1 = 6$

4.1.10 Korollar

Sei $n \in \mathbb{N}$.

$$\sum_{d|n} \varphi(d) = n.$$

Beweis: Sei G die zyklische Gruppe der Ordnung n. Jedes Element hat als Ordnung einen Teiler d von n, für jeden Teiler gibt es $\varphi(d)$ Elemente dieser Ordnung. Daher ist $\sum_{d|n} \varphi(d)$ die Anzahl der Elemente von G. $\square$

4.1.11 Satz

Für $p \geq 3$ prim und $r \in \mathbb{N}_{>0}$ ist $(\mathbb{Z}_{p^r})^*$ zyklisch.

Zur Vorbereitung:

4.1.12 Lemma

$(\mathbb{Z}_p)^*$ ist zyklisch.

Beweis: Sei $n = |\mathbb{Z}_p^*| = p-1$.

Für jeden Teiler $d | n$

sei $\Psi(d)$ die Anzahl der Elemente in $\mathbb{Z}_p^*$, die Ordnung d haben.

Wähle d mit $\Psi(d) \neq 0$.

$\Rightarrow \exists\, a \in \mathbb{Z}_p^*$, $\operatorname{ord}(a) = d$

$\Rightarrow \langle 1, a, \dots, a^{d-1} \rangle \subset \mathbb{Z}_p^*$

ist eine zyklische Untergruppe, alle ihre Elemente x erfüllen $x^d = 1$

$\Rightarrow$ Das Polynom $x^d - 1 \in \mathbb{Z}_p[X]$

hat mindestens d Nullstellen $\Rightarrow$
das Polynom $x^d - 1$ hat genau d
Nullstellen $\Rightarrow$ alle Elemente in
$\mathbb{Z}_p^*$ der Ordnung d liegen in $\langle a \rangle$
$\Rightarrow \Psi(d) \leq \varphi(d)$.

$$\Rightarrow n = \sum_{d|n} \Psi(d) \leq \sum_{d|n} \varphi(d) \overset{4.1.10}{=} n$$

$\Rightarrow \Psi(d) = \varphi(d) \quad \forall d$

$\Rightarrow \Psi(n) = \varphi(n) \neq 0 \Rightarrow \exists\, b \in \mathbb{Z}_p^*$,
$\operatorname{ord}(b) = n \Rightarrow \mathbb{Z}_p^* = \langle b \rangle$ ist
zyklisch. □

4.1.13 Lemma

Sei G eine Gruppe, $x, y \in G$,
mit $xy = yx$ und $\langle x \rangle \cap \langle y \rangle = \{e\}$.

Dann gilt
$\operatorname{ord}(xy) = \operatorname{kgV}(\operatorname{ord}(x), \operatorname{ord}(y))$.

Beweis:
Sei $\operatorname{ord}(x) = n$, $\operatorname{ord}(y) = m$, $k = \operatorname{kgV}(m,n)$.
Es gilt $(xy)^k = x^k y^k = e$
$\Rightarrow \operatorname{ord}(xy) \mid k$.

Sei l so, daß $(xy)^l = e$

$\Rightarrow x^l y^l = e \Rightarrow x^l = \left(\frac{1}{y}\right)^l$

$\in \langle x \rangle \cap \langle y \rangle = \{e\} \Rightarrow$

$x^l = e$ und $\left(\frac{1}{y}\right)^l = e \Rightarrow y^l = e$

$\Rightarrow n \mid l$ und $m \mid l$

$\Rightarrow k \mid l \Rightarrow k \mid \operatorname{ord}(xy)$

$\Rightarrow \operatorname{ord}(xy) = k.$ □

4.1.14 Lemma

$a \equiv b \bmod p^r \Rightarrow a^p \equiv b^p \bmod p^{r+1}$

Beweis: $a = b + kp^r \Rightarrow$

$a^p = (b + kp^r)^p =$

$\sum_{j=0}^{p} \binom{p}{j} b^{p-j} (kp^r)^j \equiv b^p \bmod p^{r+1}$

da $\binom{p}{1} = p.$ □

Bem Ist p prim und $0<j<p$, so gilt $p \mid \binom{p}{j}$, denn p teilt den Zähler von $\frac{p!}{j!(p-j)!} = \binom{p}{j}$ aber nicht den Nenner.

4.1.15 Lemma

Sei $p \geq 3$ prim und $r \geq 2$. Dann:

$$a \equiv 1 + p^{r-1} \bmod p^r \Rightarrow a^p \equiv 1 + p^r \bmod p^{r+1}$$

Beweis:

$$a^p \overset{4.1.14}{\equiv} (1+p^{r-1})^p = \sum_{j=0}^{p} \binom{p}{j} p^{(r-1)\cdot j}$$

$$= 1 + p \cdot p^{r-1} + \sum_{j=2}^{p} \binom{p}{j} p^{(r-1)\cdot j}$$

$$\equiv 1 + p^r \bmod p^{r+1} \qquad \square$$

Beweis von Satz 4.1.11:

Der Fall $r = 1$ ist Lemma 4.1.12.

Sei $r \geq 2$. Es gilt

$|\mathbb{Z}_{p^r}^*| = p^{r-1} \cdot (p-1)$.

Wir konstruieren Elemente $x, y \in \mathbb{Z}_{p^r}^*$ mit

$ord(\bar{x}) = p^{r-1}$, $ord(\bar{y}) = p-1$,

dann folgt mit Lemma 4.1.13 (da $ggT(p^{r-1}, p-1) = 1$ und die Elemente in $\langle \bar{x} \rangle$ und in $\langle \bar{y} \rangle$ als Ordnungen Teiler von p^{r-1} bzw. $p-1$ haben) $ord(\bar{x}\bar{y}) = p^{r-1} \cdot (p-1)$ und $\langle \bar{x}\bar{y} \rangle = \mathbb{Z}_{p^r}^*$, also ist $\mathbb{Z}_{p^r}^*$ zyklisch.

Sei $\langle \bar{b} \rangle = \mathbb{Z}_p^*$ und $d = ord(\bar{b})$ in $\mathbb{Z}_{p^r}^*$. Da dann auch $\bar{b}^d = 1$ in $\mathbb{Z}_p^*$ folgt $(p-1) \mid d$.

Für $\bar{y} = \bar{b}^{\frac{d}{p-1}}$ folgt mit dem Satz über Untergruppen zyklischer Gruppen 2.3.13 (3)

$$ord(\bar{y}) = ord\left(\bar{b}^{\frac{d}{p-1}}\right) = \frac{ord(\bar{b})}{ggT\left(ord(\bar{b}), \frac{d}{p-1}\right)} = \frac{d}{ggT\left(d, \frac{d}{p-1}\right)} =$$

$$\frac{d}{\frac{d}{p-1}} = p-1.$$

Setze $= 1+p$. Dann gilt

$$x \equiv 1+p \mod p^2 \overset{4.1.15}{\Rightarrow}$$

$$x^p \equiv 1+p^2 \mod p^3 \overset{4.15}{\Rightarrow}$$

$$x^{p^2} \equiv 1+p^3 \mod p^4 \Rightarrow \dots \Rightarrow$$

$$x^{p^{r-2}} \equiv 1+p^{r-1} \mod p^r$$

$$\Rightarrow x^{p^{r-2}} = 1+p^{r-1}+kp^r$$

$$\Rightarrow x^{p^{r-1}} = \left(1+p^{r-1}+kp^r\right)^p =$$

$$\sum_{j=0}^{p} \binom{p}{j} \left(p^{r-1} + k p^r\right)^j$$

$$= 1 + p \cdot \left(p^{r-1} + k p^r\right) + \sum_{j=2}^{p} \binom{p}{j} \left(p^{r-1} + k p^r\right)^j$$

$$= 1 + p^r \mod p^r$$

$$\equiv 1 \mod p^r$$

$$\Rightarrow \bar{y}^{p^{r-1}} = \bar{1} \text{ und } \bar{y}^{p^{r-2}} \neq \bar{1}$$

$$\Rightarrow \operatorname{ord}(\bar{y}) = p^{r-1}.$$

□

4.2 Anwendungen

4.2.1 Algorithmus (Primzahltest)

Sei $n \in \mathbb{N}$.

1) Wähle $a \in \mathbb{Z}$, bestimme $ggT(a,n)$ mit dem euklidischen Algorithmus.
Falls $ggT(a,n) \neq 1 \Rightarrow$ n nicht prim.

2) Ist $ggT(a,n) = 1$, teste ob $a^n \equiv a \mod n$. Falls nicht $\Rightarrow$ n nicht prim (Kleiner Satz von Fermat)
Sonst keine Aussage, zurück zu 1).

Der Algorithmus terminiert nicht, falls n prim ist.
Man erhennt nur Nicht-Primzahlen, mit mehr Durchläufen erhöht sich die Wahrscheinlichkeit, daß eine Zahl, die nicht als Nicht-Prim

erkannt wird, tatsächlich prim ist.

4.2.2 Def n heißt Fermatsche Pseudoprimzahl zur Basis a, falls n nicht prim ist, aber $a^n \equiv a \bmod n$.

Bsp: $2^{341} \equiv 2 \bmod 341$,
aber $341 = 11 \cdot 31$ ist keine Primzahl, sondern eine Pseudoprimzahl zur Basis 2.
Verwenden wir die Basis 3, so erhalten wir $3^{341} \equiv 168 \not\equiv 3 \bmod 341$, so können wir schließen, daß 341 keine Primzahl ist.

4.2.3 Das RSA-Verfahren
(Rivest, Shamir, Adleman)

Ein Verschlüsselungsverfahren, das darauf beruht, daß Zahlen schwer zu faktorisieren sind.
Alice möchte von Bob verschlüsselte Nachrichten empfangen können.

Vorbereitung:

I Bob:

1. Wähle eine große Zahl N und kodiere Nachrichten in Zahlen $0 \leq m < N$.

II Alice:

2. Wähle 2 Primzahlen p, q mit $pq > N$, berechne $n = pq$ und $\varphi(n) = (p-1) \cdot (q-1)$.
3. Wähle $e \in \mathbb{N}$ mit $ggT(e, \varphi(n)) = 1$.
4. Berechne das Inverse von e mod $\varphi(n)$, also $0 < d < \varphi(n)$ mit $ed \equiv 1 \mod \varphi(n)$.
5. $p, q, \varphi(n)$ kann vergessen werden.
6. (n, e) ist öffentlicher Schlüssel. Alice gibt diese Daten Bob.

   d ist Alices privater Schlüssel. Sie hält diese Zahl geheim.

Nachrichtenübertragung und Entschlüsselung

III. Bob möchte an Alice eine Nachricht senden, z.B. die Zahl m.
Er verschlüsselt mit Alices öffentlichem Schlüssel:

1. Berechne
$$c := m^e \bmod n$$

2. Sende c an Alice.

IV. Alice:
Berechne $\tilde{m} := c^d \bmod n$
mit dem geheimen Schlüssel d.
Dann gilt
$$\tilde{m} \equiv c^d \equiv (m^e)^d \equiv m^{ed} \equiv$$
$$m^{1+k\cdot\varphi(n)} \equiv m \cdot (m^{\varphi(n)})^k \equiv$$
$$m \bmod n$$
Da $m < N$ ist lässt sich m dadurch eindeutig zurück-

gewinnen.

Bem:
Um zu entschlüsseln braucht man d, also $\varphi(n)$, also die Faktorisierung pq von n.

Bsp:

$n = 7 \cdot 11 = 77$, $\varphi(n) = 6 \cdot 10 = 60$

$e = 13$,

$1 = ggT(13, 60) = (-23) \cdot 13 + 5 \cdot 60$,

also $d = -23 = 37$.

Bob verschlüsselt $m = 31$, also

$m^e \bmod n = 31^{13} \bmod 77$

$\equiv 3 \bmod 77$.

Bob sendet an Alice: 3.

Alice entschlüsselt:

$3^d = 3^{37} \equiv 31 \bmod 77$.