III

Elementare Zahlentheorie

3.1. Für $a \in \mathbb{Z} \setminus \{0\}$ sind gleichbedeutend:
(1) $\bar{a}$ ist eine Einheit im Ring $\mathbb{Z}/n\mathbb{Z}$ (multiplikativ invertierbar)
(2) $\bar{a}$ erzeugt die additive Gruppe $\mathbb{Z}/n\mathbb{Z}$
(3) a und n sind teilerfremd.

3.2. (Die Eulersche ϕ-Funktion) Wir definieren $\phi: \mathbb{N}_{\geq 1} \to \mathbb{N}_{\geq 1}$ durch
$\phi(n)$ = die Anzahl der zu n teilerfremden Zahlen in $\{1, \dots, n-1\}$
$= |(\mathbb{Z}/n\mathbb{Z})^\times|$.
(1) Sind $m, n \geq 1$ teilerfremd, so gilt $\phi(mn) = \phi(m)\phi(n)$.
(2) Ist p eine Primzahl und $k \geq 1$, dann $\phi(p^k) = (p-1)p^{k-1}$.
(3) Ist $n = p_1^{k_1} \cdots p_\ell^{k_\ell}$ die Primfaktorzerlegung von n, so gilt:
$\phi(n) = (p_1 - 1) \cdots (p_\ell - 1) p_1^{k_1 - 1} \cdots p_\ell^{k_\ell - 1}$.

3.3 (Satz von Euler) Seien $n, a \in \mathbb{Z}$ und $n \geq 1$, $a \neq 0$. Sind a und n teilerfremd, so gilt $a^{\phi(n)} \equiv 1 \bmod n$.

3.4 (Kleine Satz von Fermat) Sei p prim und $a \in \mathbb{Z}$. Dann gilt $a^p \equiv a \bmod p$.
Ist p kein Teiler von a, dann gilt $a^{p-1} \equiv 1 \bmod p$.

$a^{\phi(n)} \equiv 1 \bmod n$ } Euler
$a^{p-1} \equiv 1 \bmod p$ } Fermat
$a^p \equiv a \bmod p$

3.3 Einheitswurzeln und Kreisteilungspolynome

3.5 Sei $n \in \mathbb{N}$. Ein $\zeta \in \mathbb{C}$ mit $\zeta^n = 1$ heißt (komplexe) n-te Einheitswurzel.
$\Rightarrow$ Nullstelle des Polynoms $X^n - 1 \in \mathbb{C}[X]$.
$\Rightarrow$ Es gibt höchstens n n-te Einheitswurzeln. Form $e^{\frac{2\pi i k}{n}}$ für $k = \{0, \dots, n-1\}$.

Die Menge $\mu_n = \{\zeta \in \mathbb{C} \mid \zeta^n = 1\} = \{e^{\frac{2\pi i k}{n}} \mid k = 0, 1, \dots, n-1\}$ ist eine Untergruppe der multiplikativen Gruppe $\mathbb{C}^\times$ mit n Elementen. Die Gruppe ist zyklisch, da $e^{\frac{2\pi i k}{n}} = e^{\left(\frac{2\pi i}{n}\right)^k}$ also isomorph zu $\mathbb{Z}/n\mathbb{Z}$.

3.6. Sei $n \geq 1$ und $k \neq 0$. Dann ist $e^{\frac{2\pi i k}{n}}$ ein Erzeuger von μ_n genau dann, wenn k und n teilerfremd sind.

3.7 ϕ_d heißt d-tes Kreisteilungspolynom.

$$\phi_d(X) = \prod_{\text{ord}\,\zeta = d} (X - \zeta)$$

$$\Rightarrow X^n - 1 = \prod_{d \mid n} \phi_d(X).$$

ϕ_n für $n \geq 1$ sind irreduzibel.

Hier: $\phi_p(x) = x^{p-1} + x^{p-2} + \dots + x + 1$

$\phi_{p^2}(x) = x^{p^2-1} + x^{p^2-2} + \dots + x^{p-1} + 1$

$\phi_{p^n}(x) = 1 + x^{p^{n-1}} + x^{2p^{n-1}} + \dots + x^{(p-1)p^{n-1}}$

für n ist p-Potenz.

Die Koeffizienten von ϕ_d sind ganze Zahlen.
Allgemein gilt $X^n - 1 = (X-1)(X^{n-1} + X^{n-2} + \dots + 1)$ und damit
$\phi_p(X) = X^{p-1} + X^{p-2} + \dots + 1$ für eine Primzahl p. Insbesondere ist $\phi_d \in \mathbb{Z}[X]$.

3.10 Für alle $d \geq 1$ hat ϕ_d ganze Koeffizienten: $\phi_d \in \mathbb{Z}[X]$.

3.11 Sei p eine Primzahl. Dann ist das p-te Kreisteilungspolynom $\phi_p \in \mathbb{Q}[X]$ irreduzibel.

3.12 Eine d-te Einheitswurzel $\zeta \in \mathbb{C}$ der Ordnung d heißt primitive d-te Einheitswurzel.
Damit gilt also

$$\phi_d(X) = \prod_{\text{ord}(\zeta) = d} (X - \zeta).$$

Die primitiven d-ten Einheitswurzeln sind genau die Erzeuger der zyklischen Gruppe $\mu_d = \{\zeta \in \mathbb{C} \mid \zeta^d = 1\}$.

3.4 Endomorphismen von $\mathbb{Z}/n\mathbb{Z}$

$\mathrm{End}_{Gr}(\mu_n) = \{\phi : \mu_n \to \mu_n \mid \phi \text{ ist ein Homomorphismus von Gruppen}\}$,
die Menge der Endomorphismen von μ_n und
$\mathrm{Aut}_{Gr}(\mu_n) = \{\phi : \mu_n \to \mu_n \mid \phi \text{ ist bijektiv}\}$
die Menge der Automorphismen von μ_n.

Def: $(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{a} \mid \bar{a} \in \mathbb{Z}/n\mathbb{Z} \text{ ist multiplikativ invertierbar}\}$

Lemma: $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$. Dann sind $\bar{a} = a + n\mathbb{Z}$ äquivalent.
(1) $\bar{a}$ ist eine Einheit.
(2) $\mathrm{ord}(\bar{a}) = n$
(3) a und n sind teilerfremd.

Bsp. $n = p \Rightarrow \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ ist Körper
$\Rightarrow (\mathbb{Z}/p\mathbb{Z})^\times = \mathbb{F}_p^\times = \{x \in \mathbb{F}_p \mid x \neq 0\}$
$\Rightarrow |(\mathbb{Z}/p\mathbb{Z})^\times| = p-1$
$(\mathbb{Z}/6\mathbb{Z})^\times = \{\bar{1}, \bar{5}\}$

Frage: Wie viele Elemente hat $(\mathbb{Z}/n\mathbb{Z})^\times$?

Def.: Definiere $\varphi : \mathbb{N}_{\geq 1} \to \mathbb{N}_{\geq 1}$
$\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$ = Anzahl der zu n teilerfremden $a \in [0, 1, \dots, n-1]$
Also $\varphi(p) = p-1$ falls p prim ist.

Satz: (1) Falls $\mathrm{ggT}(m,n) = 1$, $\varphi(mn) = \varphi(m)\varphi(n)$
(2) $\varphi(p^k) = (p-1)p^{k-1}$, falls p prim und $k \geq 1$
(3) $\varphi(n) = (p_1-1)(p_2-1)\cdots(p_r-1)p_1^{k_1-1}\cdots p_r^{k_r-1}$
falls $n = p_1^{k_1}\cdots p_r^{k_r}$ die Primfaktorzerlegung von n ist.

Bem.: $(\mathbb{Z}/n\mathbb{Z})^\times$ ist eine Gruppe mit der Multiplikation.
! Keine Gruppe unter Addition i. A.

Satz von Euler: $n \in \mathbb{N}_{\geq 1}$, $a \in \mathbb{Z}$. Gilt $\mathrm{ggT}(a,n) = 1$
$\Rightarrow a^{\varphi(n)} \equiv 1 \bmod n$.

Erweiterte euklidische Algorithmus

R ist ein euklidischer Ring mit $d: R \setminus \{0\} \to \mathbb{N} = \{0, 1, 2, \dots\}$
Für $a, b \in R$, $a \neq 0$ gibt es r, s:
1) $b = r \cdot a + c$
2) $d(c) < d(a)$ oder $c = 0$.

Algorithmus: Gegeben $a, b \in R$, $a \neq 0$

$\to b = c_0 \cdot a + r_0$ $\quad d(r_0) < d(a)$ oder $r_0 = 0$
$\to a = c_1 r_0 + r_1$ $\quad d(r_1) < d(r_0)$ oder $r_1 = 0$
$\to r_0 = c_2 r_1 + r_2$ $\quad d(r_2) < d(r_1)$ oder $r_2 = 0$
$\to r_{n-3} = c_{n-1} r_{n-2} + r_{n-1}$ ...
$\to r_{n-2} = c_n r_{n-1} + 0$ $\quad$ also $r_n = 0$

Beh.: r_{n-1} ist ggT von a und b.

Irreduzibilitätskriterium

Sei K ein Körper.
$P(X) \in K[x]$ Polynom vom Grad ≤ 3.
Dann ist $P(x)$ irreduzibel genau dann, wenn P in K keine Nullstelle hat.

Das quadratische Reziprozitätsgesetz

Sei p eine Primzahl und $P(x) = ax^2 + bx + c \in \mathbb{F}_p[x]$
Frage: Hat p in $\mathbb{F}_p$ eine Nullstelle?
1. Reduktion: können $a = 1$ annehmen
2. Reduktion: (quadratische Ergänzung) können $b = 0$ annehmen, falls $p \neq 2$.

$$x^2 + bx + c = \left(x + \frac{1}{2}b\right)^2 + c - \frac{1}{4}b^2$$

(falls $p = 2$: leicht zu lösen durch Ausprobieren)
$x = 0$: $c = 0$
$x = 1$: $a + b + c = 0$

Def: (1) $c \in \mathbb{F}_p$ heißt quadratischer Rest falls es ein $a \in \mathbb{F}_p$ gibt mit $a^2 = c$.
(2) $c \in \mathbb{Z}$ heißt quadratischer Rest mod. p, falls es ein $a \in \mathbb{Z}$ gibt mit $a^2 \equiv c \bmod p$.

Bem: Es gibt in $\mathbb{F}_p$ genau $\frac{p-1}{2}$ Quadrate $\neq 0$ und $\frac{p-1}{2}$ viele Quadrate

$$\mathbb{F}_p = \left\{ \begin{matrix} \text{Quadrate} \\ \text{in } \mathbb{F}_p^\times \end{matrix} \right\} \cup \{0\} \cup \left\{ \begin{matrix} \text{Nicht Quadrate} \\ \text{in } \mathbb{F}_p^\times \end{matrix} \right\}^2 \qquad \frac{p-1}{2} + 1 + \frac{p-1}{2} = p.$$

Legendre-Symbol

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

$$\left(\frac{a}{p}\right) := \begin{cases} 1, & \text{falls } a \text{ quad. Rest mod } p \text{ und } p \nmid a. \\ 0, & \text{falls } p \mid a \\ -1, & \text{falls } p \nmid a \text{ und } a \text{ kein quad. Rest mod. } p. \end{cases}$$

Bsp. $p = 5$

a	0	1	2	3	4
$\left(\frac{a}{p}\right)$	0	1	-1	-1	1

$p = 11$

a	0	1	2	3	4	5	6	7	8	9	10
$\left(\frac{a}{p}\right)$	0	1	-1	1	1	1	-1	-1	-1	1	-1

Satz zum quadratischen Reziprozitätsgesetz:

p, q verschiedene Primzahlen $\neq 2$. $\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

Def: Sei $a \in \mathbb{Z}$ mit $p \nmid a$. Dann heißt a quadratischer Rest mod. p, falls es ein $x \in \mathbb{Z}$ gibt $x^2 \equiv a \bmod p$. Ansonsten heißt a quadratischer Nichtrest mod. p.

Satz: $p > 2$ prim
a) $a \equiv b \bmod p \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$
b) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$
c) Das Legendresymbol definiert einen Gruppenhom.
$L : \mathbb{F}_p^\times \to \{\pm 1\} \cong \mathbb{Z}/2\mathbb{Z}$, $[x] \mapsto \left(\frac{x}{p}\right)$

Satz: (Eulerkriterium) $p > 2$ prim, $a \in \mathbb{Z}$
Dann gilt $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p$.

Erster Ergänzungssatz: $p>2$ prim. Dann gilt

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, & p \equiv 1 \bmod 4 \\ -1, & p \equiv 3 \bmod 4. \end{cases}$$

Halbsysteme

$p \neq 2 \Rightarrow a \neq -a$ für alle $a \in \mathbb{F}_p^\times$.

Def.: Ein Halbsystem mod. p ist eine Teilmenge $S \subseteq \mathbb{F}_p^\times$ die für alle $a \in \mathbb{F}_p^\times$ genau ein Element aus $\{+a, -a\}$ enthält. ($a \in S \Leftrightarrow -a \notin S$)

Bsp.: $S = \{\bar{1}, \bar{2}, \dots, \overline{\frac{p-1}{2}}\} \subseteq \mathbb{F}_p^\times$

$\mathbb{F}_p^\times$: $\bar{1}$ $\bar{2}$ $\bar{3}$ $\dots$ $\overline{\frac{p-1}{2}}$ $\overline{\frac{p+1}{2}}$ $\dots$ $\overline{p-2}$ $\overline{p-1}$

$\overline{\frac{p+1}{2}} = -\overline{\frac{p-1}{2}}$, $\overline{p-2} = -\bar{2}$, $\overline{p-1} = -\bar{1}$

$-a = \overline{p-a}$

Lemma von Gauß: $p>2$ prim, $S \subseteq \mathbb{F}_p^\times$ Halbsystem.
Sei $a \in \mathbb{Z}$, $p \nmid a$. Dann ist auch $aS := \{\overline{ax} \mid \bar{x} \in S\}$ ein Halbsystem mod. p und $\left(\frac{a}{p}\right) = (-1)^{|(-S) \cap (aS)|}$.

Zweiter Ergänzungssatz: $p>2$ prim.

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & p \equiv \pm 1 \bmod 8 \\ -1, & p \equiv \pm 3 \bmod 8. \end{cases}$$

($p^2-1 = (p-1)(p+1)$ durch 8 teilbar; $\frac{p^2-1}{8}$ gerade $\Leftrightarrow$ $p-1$ oder $p+1$ durch 8 teilbar)

Quadratisches Reziprozitätsgesetz

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \left(\frac{q}{p}\right)$$

$p \neq q$ seien ungerade Primzahlen.
Dann gilt

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} = \begin{cases} 1, & \text{falls } p \equiv 1 \bmod 4 \text{ oder } q \equiv 1 \bmod 4 \\ -1, & \text{falls } p \equiv 1 \bmod 4 \text{ und } q \equiv 1 \bmod 4. \end{cases}$$

Lemma: Sei $a \in \mathbb{Z}$, $a \geq 1$, $p>2$ prim und $p \nmid a$. Dann ist

$$\left(\frac{a}{p}\right) = (-1)^h \text{ wobei } h = \left|\left\{(x,y) \in \mathbb{Z}^2 \mid 0<x<\tfrac{p+1}{2},\ 0<y<\tfrac{q+1}{2},\ -\tfrac{p}{2} < ax - py < 0\right\}\right|.$$

⚠ **Satz (Jacobi-Symbol):** $a, b, m, n \in \mathbb{Z}$, $m, n \geq 1$ ungerade:

a) Wertebereich: $\left(\frac{a}{n}\right) \in \{0, 1, -1\}$

b) $\left(\frac{a}{n}\right) = 0 \Leftrightarrow \operatorname{ggT}(a,n) \neq 1$

c) $a \equiv b \bmod n \Rightarrow \left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$

d) $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$

e) $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$, $\left(\frac{a}{p_1^{\alpha_1}\cdots p_n^{\alpha_n}}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \cdots \left(\frac{a}{p_n}\right)^{\alpha_n}$

f) 1. Ergänzungssatz: $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$, $\left(\frac{-1}{p}\right) = \begin{cases} 1, & p \equiv 1 \bmod 4 \\ -1, & p \equiv -1 \bmod 4. \end{cases}$

g) 2. Ergänzungssatz: $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$, $\left(\frac{2}{p}\right) = \begin{cases} 1, & p \equiv \pm 1 \bmod 8 \\ -1, & p \equiv \pm 3 \bmod 8 \end{cases}$

h) $\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}$

i) n prim, $n \nmid a$: $\left(\frac{a}{n}\right) = 1$

$\Leftrightarrow$ a quadr. Rest mod. n $\Leftrightarrow$ $x^2 = \bar{a}$ lösbar in $\mathbb{F}_n$