Zusammenfassung zu Zahlentheorie

Sara Adams

11. Juli 2004

Diese Zusammenfassung basiert auf der Vorlesung
Zahlentheorie
gehalten im Sommersemester 2004
von Prof. Dr. Klaus Metsch
an der Justus-Liebig Universität Gießen

Inhaltsverzeichnis

1 Teilbarkeit ganzer Zahlen

1.1 Teilbarkeit

Definitionen

- $t, z \in \mathbb{Z}, t \neq 0$ Dann: $t|z :\Leftrightarrow \exists\, x \in \mathbb{Z}:\ tx = z$ (t Teiler von z, z Vielfaches von t)
- t gemeinsamer Teiler von $a, b \in \mathbb{Z} :\Leftrightarrow\ t|a \wedge t|b$
- t ggT von $a, b \in \mathbb{Z}, a \neq 0 \vee b \neq 0 \Leftrightarrow t = (a, b) :\Leftrightarrow\ t|a \wedge t|b, \nexists s > t:\ s|a \wedge s|b$
- v gemeinsames Vielfaches von $a, b \in \mathbb{Z}\backslash\{0\} :\Leftrightarrow\ a|v \wedge b|v$
- v kgV von $a, b \in \mathbb{Z}\backslash\{0\} \Leftrightarrow v = [a, b] :\Leftrightarrow\ a|v \wedge b|v, \nexists w < v:\ a|w \wedge b|w$

Sätze

- $t, t_1, t_2, a, b \in \mathbb{Z}$
  - $t|a,\ t|b \Rightarrow\ t|(a + b)$
  - $t|a \Rightarrow\ t|ab$
  - $t_1|a,\ t_2|b \Rightarrow\ t_1t_2|ab$
- Division mit Rest: $a, t \in \mathbb{Z}, t \geq 1 \Rightarrow\ \exists!\, b, r \in \mathbb{Z}:\ a = bt + r, \quad 0 \leq r \leq t - 1$
- $r_1, r_2, r_3, t \in \mathbb{N}, r_1 = r_2t + r_3 \Rightarrow\ (r_1, r_2) = (r_2, r_3)$
- Euklidischer Algorithmus: Zurückführen des ggT auf kleinere Zahlen mit Abbruchkriterium "Division liefert Rest 0"
- $a, b \in \mathbb{Z}\backslash\{0\} \Rightarrow\ \exists x, y \in \mathbb{Z}:\ ax + by = (a, b)$
- $a, b \in \mathbb{Z}\backslash\{0\}:\ t \in \mathbb{Z}$ Teiler von $a, b \Leftrightarrow\ t|(a, b)$
- $a, b \in \mathbb{N}:\ (a, b) \cdot [a, b] = ab$
- $a, b \in \mathbb{Z}\backslash\{0\}:\ w$ gemeinsames Vielfaches von $a, b \Leftrightarrow\ [a, b]|w$

1.2 Primzahlen

Definitionen

- $p \in \mathbb{N}$ Primzahl $:\Leftrightarrow$ 1 und p sind die einzigen Teiler von p in $\mathbb{N}$
- $a, b \in \mathbb{Z}\backslash\{0\}$ teilerfremd $:\Leftrightarrow\ (a, b) = 1$
- p Fermatsche Primzahl $:\Leftrightarrow\ p = 2^n + 1$

Sätze

- Fundamentalsatz der elementaren Zahlentheorie: Jede natürliche Zahl $n > 1$ lässt sich bis auf Reihenfolge der Faktoren eindeutig als Produkt von Primzahlen schreiben.
- $a_1, ..., a_s \in \mathbb{Z}, p$ Primzahl, $p|a_1 \cdot ... \cdot a_s \Rightarrow\ \exists i:\ p|a_i$
- Es gibt unendlich viele Primzahlen.
- $t_1, ..., t_r$ paarweise teilerfremd, $a \in \mathbb{N}, t_i|a\ \forall i \Rightarrow\ t_1 \cdot ... \cdot t_r|a$

1.3 Vollkommene Zahlen

Definitionen

- $n \in \mathbb{N}:\ \sigma(n) := \sum_{\mathbb{N} \ni d|n} d$
- $n \in \mathbb{N}$ vollkommen $:\Leftrightarrow\ \sigma(n) = 2n$
- Mersenne-Zahlen: $M_n := 2^n - 1$ für $n \in \mathbb{N}$

Sätze

- $\mathbb{N} \ni n = \prod_{i=1}^{s} p_i^{\nu_i}, p_i$ versch. Primzahlen $\Rightarrow\ \sigma(n) = \prod_{i=1}^{s} \frac{p_i^{\nu_i+1}-1}{p_i-1}$
- $n, m \in \mathbb{N}:\ (n, m) = 1 \Rightarrow\ \sigma(nm) = \sigma(n)\sigma(m)$
- $n \in 2\mathbb{N}$ vollkommen $\Leftrightarrow\ n = 2^{p-1}(2^p - 1),\ M_p$ Mersenne'sche Primzahlen

2 Kongruenzen

2.1 Modulo-Rechnen

Definitionen

- a kongruent b modulo $n \Leftrightarrow\ a \equiv b \bmod n :\Leftrightarrow\ n|a - b$
- $\overline{a} = \{b:\ b \equiv a\ (n)\}$ Restklasse modulo n
- $\mathbb{Z}_n := \{\overline{0}, ..., \overline{n-1}\}$ Menge aller Restklassen
- $M = \{m_1, ..., m_n\} \subset \mathbb{N}$ vollständiges Restsystem modulo $n\ \Leftrightarrow\ \mathbb{Z}_n = \{\overline{m_1}, ..., \overline{m_n}\}$
- $\overline{a} + \overline{b} := \overline{a + b} \qquad \overline{a} \cdot \overline{b} := \overline{a \cdot b}\ \Rightarrow\ \mathbb{Z}_n$ Ring
- $\mathbb{Z}_n^* = \{\overline{a} : \exists \overline{b}:\ \overline{a}\overline{b} = \overline{1}\}$ Einheitengruppe von $\mathbb{Z}_n$
- $\overline{a} \in \mathbb{Z}_n^*$ prime Restklasse modulo n

Sätze

- $\equiv$ ist eine Äquivalenzrelation
- $a \equiv a' \mod n, b \equiv b' \mod n \Rightarrow a+b \equiv a'+b' \mod n, \quad ab \equiv a'b' \mod n$
- $\mathbb{Z}_n^*$ ist multiplikative Gruppe.

2.2 Der chinesische Restsatz

- **Chinesischer Restsatz**: $r_1, ..., r_k \in \mathbb{Z}, m_1, ..., m_k \in \mathbb{N}$ pw. teilerfremd, $m_i > 1 \Rightarrow$ das System $x \equiv r_i \mod m_i \quad 1 \leq i \leq k$ hat Lösung in $\mathbb{Z}$, eindeutig modulo $m_1 \cdot ... \cdot m_k$
- **Kürzungsregel** Für $m \in \mathbb{N}, \ a,b,c \in \mathbb{Z}$ gilt: $ac \equiv bc\ (m) \Leftrightarrow a \equiv b \mod \frac{m}{(c,m)}$
- $ax \equiv b \mod n$ lösbar $\Leftrightarrow (a,n)|b$
- $ax \equiv b \mod n$ lösbar $\Rightarrow \exists$ genau (a,n) verschiedene Lösungen modulo n

2.3 Die Eulersche φ-Funktion

- **Eulersche φ-Funktion**: $\varphi(1) = 1, \ \varphi(n) = |\mathbb{Z}_n^*|$ für $n \geq 2$
- $\overline{a}$ prime Restklasse modulo $n \Leftrightarrow (a,n) = 1$
- $m,n \in \mathbb{N}, \ (m,n) = 1 : \ \varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$
- $n = \prod_{i=1}^{s} p_i^{e_i}, \ p_i \in \mathbb{P}$ pw. versch., $e_i \in \mathbb{N} \Rightarrow \varphi(n) = \prod_{i=1}^{s} p_i^{e_i-1}(p_1 - 1) = n \cdot \prod_{i=1}^{s}(1 - \frac{1}{p_i})$
- $n \in \mathbb{N} : \ \sum_{d|n} \varphi(d) = n$

2.4 Wilson, Fermat und Euler

- **Wilson**: $n \in \mathbb{N}$ Primzahl $\Leftrightarrow (n-1)! \equiv -1 \mod n$
- **Euler**: $a,n \in \mathbb{N}, \ (a,n) = 1 \Rightarrow a^{\varphi(n)} \equiv 1 \mod n$
- **kleiner Satz von Fermat**: $p \in \mathbb{P} \Rightarrow a^p \equiv a \mod p \quad \forall a \in \mathbb{Z}$
- $m \in \mathbb{N}, \ \exists a \in \mathbb{Z} : a^m \not\equiv a \mod m \Rightarrow a \notin \mathbb{P}$
- **Carmichael-Zahlen**: Zahlen $m \in \mathbb{N} \backslash \mathbb{P} : \ a^m \equiv a \mod m \quad \forall a \in \mathbb{Z}$
  Beispiele: $561 = 3 \cdot 11 \cdot 17, \ 1729 = 7 \cdot 13 \cdot 19, \ F_{13} = 2^{2^{13}} + 1$
- $p \in \mathbb{P}, \ 1 \leq j \leq p-1 \Rightarrow p|\binom{p}{j}$

2.5 Restklassenring als direkte Summe

Sei G eine multiplikativ geschriebene, endliche Gruppe.

Vorbemerkungen

- n **Ordnung** von $g \in G :\Leftrightarrow \ n \in \mathbb{N} : \ g^n = 1, [m \in \mathbb{N}, \ g^m = 1 \Rightarrow \ m \geq n]$
- G endliche, abelsche Gruppe: e **Exponent** von $G :\Leftrightarrow \ e = max\{Ord(g) : \ g \in G\}$
  - e Exponent von $G \Rightarrow \ g^e = 1 \quad \forall g \in G$
  - d Ordnung von $g \in G \Rightarrow \ d|e$
- einige Eigenschaften
  - $g^{|G|} = 1 \quad \forall g \in G$
  - $Ord(g) = c, \ n \in \mathbb{Z} : \ g^n = 1 \Leftrightarrow \ c|n$
  - $Ord(g) = n \Rightarrow \ Ord(g^c) = \frac{n}{(c,n)}$
  - $Ord(g) = n \Rightarrow \ [g^i = g^j \Leftrightarrow \ n|i-j]$
  - $Ord(g) = n \Rightarrow \ g^{-1} = g^{n-1}$
  - $Ord(g) = n, \ d|n \Rightarrow$ in $< g >$ gibt es genau $\varphi(d)$ Elemente der Ordnung d
- $G_1, ..., G_s$ multiplikativ geschriebene Gruppen $\Rightarrow \ G_1 \times ... \times G_s$ Gruppe durch:

$$(g_1, ..., g_s) \cdot (h_1, ..., h_s) := (g_1 h_1, ..., g_s h_s)$$

- $R_1, ..., R_s$ Ringe $\Rightarrow \ R_1 \times ... \times R_s$ Ring durch:

$$(r_1, ..., r_s) + (r_1', ..., r_s') := (r_1 + r_1', ..., r_s + r_s')$$
$$(r_1, ..., r_s) \cdot (r_1', ..., r_s') := (r_1 r_1', ..., r_s r_s')$$

Sätze

- $n = 2^r, \ r \in \mathbb{N} \Rightarrow [\mathbb{Z}_n^*$ zyklisch $\Leftrightarrow \ r \in \{1,2\}]$
- $n = p^r, r \in \mathbb{N}, p > 2$ Primzahl $\Rightarrow \ \mathbb{Z}_n^*$ zyklisch
- $n = \prod_{i=1}^{s} n_i, n_i \in \mathbb{N}$ pw. teilerfremd $\Rightarrow \ \mathbb{Z}_n \simeq \bigoplus_{i=1}^{s} \mathbb{Z}_{n_i}$
- $n = \prod_{i=1}^{s} n_i, n_i \in \mathbb{N}$ pw. teilerfremd $\Rightarrow \ \mathbb{Z}_n^* \simeq \mathbb{Z}_{n_1}^* \times ... \times \mathbb{Z}_{n_s}^*$
- G, H abelsche, multiplikative Gruppen: $G \times H$ zyklisch $\Leftrightarrow \ G, H$ zyklisch, $(|G|, |H|) = 1$
- $\mathbb{Z}_n^*$ zyklisch $\Leftrightarrow \ (n \in \{1,2,4\}) \vee (n = p^r) \vee (n = 2 \cdot p^r), \ 3 \leq p \in \mathbb{P}, r \in \mathbb{N}$
- G multiplikativ geschriebene Gruppe, $n := |G|$
  - $n = p^r, \ 3 \leq p \in \mathbb{P} \Rightarrow \ e = \phi(n)$
  - $n \in \{1,2,4\} \Rightarrow \ e = \phi(n)$
  - $n = 2^r, r \geq 3 \Rightarrow \ e = 2^{r-2} \neq \phi(n)$
- e_i Exponenten der Gruppen $G_i \Rightarrow \ e := [e_1, ..., e_n]$ Exponent von $G := G_1 \times ... \times G_n$

2.6 Carmichael-Zahlen

- $n \in \mathbb{N}$ zusammengesetzt:
  $a^n \equiv a \mod n \quad \forall a \in \mathbb{N}$
  $\Leftrightarrow \quad a^{n-1} \equiv 1 \mod n \quad \forall a \in \mathbb{N}, (a,n) = 1$
  $\Leftrightarrow$ Karselts Kriterium: $n = \prod_{i=1}^{s} p_i,\ s \geq 3, p_i \in \mathbb{P}$ pw. verschieden, $p_i - 1 | n-1$
  $\Leftrightarrow \quad a^n \equiv a \mod n \quad \forall a \in \mathbb{N}$
- $u \in \mathbb{N}, p_1 := 6u+1, p_2 := 12u+1, p_3 := 18u+1$ Primzahlen $\Rightarrow$ $p_1 p_2 p_3$ Carmichael-Zahl

2.7 Der Miller-Rabin-Test

Definitionen

$n \in 2\mathbb{N}+1,\ n-1 = 2^l \cdot t,\ \ l \in \mathbb{N},\ t \in 2\mathbb{N}_0+1,\ a \in \mathbb{Z}:\ (a,n) = 1$

- n erfüllt den **Miller-Rabin-Test** zur Basis $a :\Leftrightarrow \quad b := a^t, (b \equiv 1 \mod n) \vee (\exists i \in \{0,...,l-1\}:\ b^{2^i} \equiv -1 \mod n)$
- n **starke Pseudoprimzahl** zur Basis $a :\Leftrightarrow$ n erfüllt den Miller-Rabin-Test
- n **Pseudoprimzahl** zur Basis $a :\Leftrightarrow$ $a^{n-1} \equiv 1 \mod n$

Sätze

- $2 < p \in \mathbb{P},\ p-1 = 2^l \cdot t,\ l \in \mathbb{N},\ t \in 2\mathbb{N}_0+1,\ b := a^t \Rightarrow$
  $(b \equiv 1 \mod p) \vee (\exists i \in \{0,...,l-1\}:\ b^{2^i} \equiv -1 \mod p)$
- G zyklische Gruppe, $|G| = m, h \in \mathbb{N} \Rightarrow$ $\exists!$ (h,m) Elemente g mit $g^h = 1$
- $n \in 2\mathbb{N}+1 \Rightarrow$ Wahrscheinlichkeit(Miller-Rabin-Test für n falsch)$\leq \frac{1}{4}$

3 Zahlentheoretische Funktionen

3.1 Faltung

Definitionen

- **zahlentheoretische Funktion**: $f : \mathbb{N} \to \mathbb{C}$
- $Z := \{f :\ f$ zahlentheoretische Funktion$\}$
- $f \in Z$ **streng multiplikativ** $:\Leftrightarrow$ $f(m \cdot n) = f(m) \cdot f(n) \quad \forall m,n \in \mathbb{N}$
- $f \in Z$ **multiplikativ** $:\Leftrightarrow$ $f(m \cdot n) = f(m) \cdot f(n) \quad \forall m,n \in \mathbb{N} :\ (m,n) = 1$
- $f, g \in Z, c \in \mathbb{C}$:
  - $(f+g) : \mathbb{N} \to \mathbb{C}, n \mapsto f(n) + g(n)$
  - $(f * g) : \mathbb{N} \to \mathbb{C}, n \mapsto \sum_{d|n} f(d) \cdot g(\frac{n}{d})$
  - $c \cdot f : \mathbb{N} \to \mathbb{C}, n \mapsto c \cdot f(n)$
- $f \in Z_1 := \{f \in Z :\ f(1) \neq 0\} \Rightarrow$ $\exists!$ $\check{f} \in Z_1 :\ f * \check{f} = \check{f} * f = \varepsilon$

Beispiele für multiplikative Funktionen

- $\sigma :\quad \sigma(n)$, die Teilersumme von n
- Eulersche φ-Funktion
- $\tau(n) :=$ # der Teiler von $n \in \mathbb{N}$
- $\underline{0} :\quad \underline{0}(n) = 0\ \forall n \in \mathbb{N}$
- $\varepsilon :\quad \varepsilon(0) = 1,\ \varepsilon(n) = 0\ \forall n \geq 2$
- $\iota :\quad \iota(n) = n\ \forall n \in \mathbb{N}$
- $\iota_\alpha :\quad \iota_\alpha(n) = n^\alpha$
- Möbius'sche μ-Funktion: rekursive Definition: $\mu(1) = 1,\ \mu(n) = -\sum_{d|n, d \neq n} \mu(d)$

Sätze

- $(Z, +, \cdot)$ ist ein $\mathbb{C}$-Vektorraum
- $(Z, +, *)$ ist ein Integritätsbereich: für $f, g, h \in Z$ gilt:
  - $f * g = g * f$
  - $f * \varepsilon = f$
  - $(f * g) * h = f * (g * h)$
  - $f, g \neq \underline{0} \Rightarrow\ f * g \neq \underline{0}$
- $f \in Z :\quad \exists g \in Z :\ f * g = \varepsilon \Leftrightarrow\ f(1) \neq 0$
- Z_1 ist bzgl. $*$ eine kommutative Gruppe mit Einselement ε.
- $\underline{0} \neq f \in Z :\quad f$ multiplikativ $\Leftrightarrow\ f(n) = \prod_{p \in \mathbb{P}} f(p^{v_p(n)}) \quad \forall n \in \mathbb{N}, f(1) = 1$
- $f, g \in M \Rightarrow\ f * g \in M$
- $f \in M \backslash \{\underline{0}\} \Rightarrow\ f(1) = 1, f \in Z_1, \check{f} \in M$

3.2 Möbiusinversion

Sätze

- $\mu * \iota_0 = \varepsilon, \quad \mu = \check{\iota_0}$
- $f, F \in Z$:
  $F(n) = \sum_{d|n} f(d) \Leftrightarrow\ f(n) = \sum_{d|n} \mu(\frac{n}{d}) F(d)$ **Möbius'sche Umkehrformel**
- $\mu \in M,\ \mu(n) = \begin{cases} (-1)^d & n \text{ Produkt von } d \text{ versch. Primzahlen} \\ 0 & \text{sonst} \end{cases}$
- $\varphi(n) = \sum_{d|n} d\mu(\frac{n}{d})$
- $a_n :=$ # der irred. Polynome vom Grad n über $GF(q) :\quad a_n = \frac{1}{n} \sum_{d|n} q^d \mu(\frac{n}{d})$

3.3 Verallgemeinerung der Eulerschen φ-Funktion

Definitionen

- $\alpha \in \mathbb{R}:\ \sigma_\alpha := \iota_0 * \iota_\alpha, n \mapsto \sum_{d|n} d^\alpha$
- $\alpha \in \mathbb{R}:\ \psi_\alpha := \mu * \iota_\alpha, n \mapsto \sum_{d|n} \mu(\frac{n}{d}) d^\alpha$
- **Jordan'sche Veralgemeinerungen der Eulerschen φ-Funktion**: $\alpha \in \mathbb{N}:\ \varphi_\alpha(n) := \left|\{(l_1,..,l_\alpha):\ 1 \le l_i \le n, (l_1,..,l_\alpha,n) = 1\}\right|$

Sätze

- $\sigma_0 = \tau,\ \sigma_1 = \sigma,\ \sum_{d|n} \psi_\alpha(d) = (\iota_0 * \psi_\alpha)(n) = \iota_\alpha(n) = n^\alpha$
- $\alpha \in \mathbb{N}:\ \psi_\alpha = \varphi_\alpha$
- $\varphi_\alpha, \alpha \in \mathbb{N}$ hat folgende Eigenschaften:
  - φ_α ist multiplikativ
  - $\forall n \in \mathbb{N}:\ \varphi_\alpha(n) = n^\alpha \prod_{p|n, p\in\mathbb{P}} (1 - p^{-\alpha})$
  - $\sum_{d|n} \varphi_\alpha(d) = n^\alpha$
  - $\sum_{d|n} \mu(\frac{n}{d}) d^\alpha = \varphi_\alpha(n)$
  - $n \in \mathbb{N}$ Primzahl $\Leftrightarrow\ \varphi_\alpha(n) = n^\alpha - 1$

3.4 Die Riemann'sche Zetafunktion

Definitionen

- **Riemann'sche ζ-Funktion**: $\zeta : \{s \in \mathbb{C}:\ \Re(s) > 1\} \to \mathbb{C}, s \mapsto \sum_{n=1}^\infty n^{-s}$
- g beschränkt, zahlentheoretisch: $G(s) := \sum_{n=1}^\infty g(n) n^{-s}$

Sätze

- $f \in M, \sum_{n=1}^\infty f(n)$ absolut konvergent $\Rightarrow\ \sum_{n=1}^\infty f(n) = \prod_{p\in\mathbb{P}} \sum_{\nu=0}^\infty f(p^\nu)$
- $\zeta(s) = \prod_{p\in\mathbb{P}} \sum_{\nu=0}^\infty p^{-\nu s} = \prod_{p\in\mathbb{P}} (1 - p^{-s})^{-1}$
- $g \in M$ beschränkt $\Rightarrow\ G(s) = \prod_{p\in\mathbb{P}} \sum_{\nu=0}^\infty g(p^\nu) p^{-\nu s}$
- $\sum_{n=1}^\infty \mu(n) n^{-s} = \frac{1}{\zeta(s)}$
- $\sum_{\mathbf{n=1}}^\infty \frac{\mu(\mathbf{n})}{\mathbf{n^2}} = \frac{\mathbf{6}}{\pi^\mathbf{2}}$

3.5 Wahrscheinlichkeit für Teilerfremdheit

Definitionen

- Seien $g, f : \mathbb{R} \to \mathbb{R},\ g(x) > 0 \forall x$:
  - $f(x) = O\big(g(x)\big), x \to \infty :\Leftrightarrow\ \frac{f(x)}{g(x)}$ beschränkt für $x > x_0$
  - $f(x) = o\big(g(x)\big), x \to \infty :\Leftrightarrow\ \lim_{x\to\infty} \frac{f(x)}{g(x)} = 0$
  - $f(x) \sim g(x), x \to \infty :\Leftrightarrow\ \lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$

Sätze

- $\sum_{n\le x} \varphi(n) - \frac{3}{\pi^2} x^2 = O(x \log x)$
- $x \in \mathbb{R}^+,\ \pi(x) := \left|\{p \in \mathbb{P}:\ p \le x\}\right| \Rightarrow\ \pi(x) \sim \frac{x}{\log(x)}$

4 Das quadratische Reziprozitätsgesetz

4.1 Das Legendre-Symbol

Definitionen

- $p \in \mathbb{P},\ p > 2,\ a \in \mathbb{Z}:$
  - a **quadratischer Rest mod** $p :\Leftrightarrow\ p \not| a,\ \exists b \in \mathbb{Z}:\ a \equiv b^3 \mod p$
  - a **quadratischer Nichtrest mod** $p :\Leftrightarrow\ p \not| a,\ \forall b \in \mathbb{Z}:\ a \not\equiv b^3 \mod p$
- **Legendre-Symbol** $\left(\frac{c}{p}\right) := \begin{cases} 1 & \text{falls } c \text{ quadratischer Rest } \mod p \\ 0 & \text{falls } p|c \\ -1 & \text{falls } c \text{ quadratischer Nichtrest } \mod p \end{cases}$

Sätze

- $p \in \mathbb{P}, p > 2,\ a_1, a_2 \in \mathbb{Z}:$
  - a_1, a_2 quad. Reste $\mod p \Rightarrow\ a_1 \cdot a_2$ quad. Rest $\mod p$
  - a_1 quad. Rest $\mod p,\ a_2$ quad. Nichtrest $\mod p \Rightarrow\ a_1 \cdot a_2$ quad. Nichtrest $\mod p$
  - a_1, a_2 quad. Nichtreste $\mod p \Rightarrow\ a_1 \cdot a_2$ quad. Rest $\mod p$
  - $\left|\{a \in \mathbb{Z}_p:\ a \text{ quad. Rest}\}\right| = \left|\{a \in \mathbb{Z}_p:\ a \text{ quad. Nichtrest}\}\right| = \frac{p-1}{2}$
- $c \equiv c' \mod p \Rightarrow\ \left(\frac{c}{p}\right) = \left(\frac{c'}{p}\right)$
- $p \in \mathbb{P}, p > 2,\ a \in \mathbb{Z}:\ \mathrm{Ord}(a) = p - 1 \Rightarrow\ \left(\frac{a^r}{p}\right) = (-1)^r$
- $p \in \mathbb{P}\backslash\{2\}:\ \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

4.2 Das quadratische Reziprozitätsgesetz

Definitionen

- $n \in 2\mathbb{N}+1, \mathbb{Z}_n = \{0, x_1, -x_1, .., x_{\frac{n-1}{2}}, -x_{\frac{n-1}{2}}\}$: H **Halbsystem** mod $n :\Leftrightarrow$ $H = \{(x_1 \text{ xor } -x_1), .., (x_{\frac{n-1}{2}} \text{ xor } -x_{\frac{n-1}{2}})\}$
- $H = \{h_1, .., h_{\frac{n-1}{2}}\}$ Halbsystem: $\{-h_1, -h_{\frac{n-1}{2}}\}$ **komplementäres Halbsystem** mod n
- H, H' komplementäre Halbsysteme, $x \in \mathbb{Z}_n \backslash \{0\}$:
  $\varepsilon_x(y) := \begin{cases} 1 & \text{falls } \{x, x\cdot y\} \subset H \vee \{x, x\cdot y\} \subset H' \\ -1 & \text{sonst} \end{cases}$
- $n \in 2\mathbb{N}+1,\ y \in \mathbb{Z}_n^*, H$ Halbsystem mod n : $\chi_n(y) := \prod_{x\in H} \varepsilon_x(y)$ (wohldefiniert)
- $m \in \mathbb{Z}, n \in 2\mathbb{Z}+1$: **Jacobi-Symbol** $(\frac{m}{n}) := \begin{cases} \chi_n(m+n\mathbb{Z}) & (m,n)=1 \\ 0 & \text{sonst} \end{cases}$
- $x \in \mathbb{R}, z := \lfloor x \rfloor$: $R(x) := \begin{cases} x-z & x < z+\frac{1}{2} \\ 0 & x = z+\frac{1}{2} \\ x-(z+1) & x > z+\frac{1}{2} \end{cases}$

Sätze

- $n \in 2\mathbb{N}+1, x \in \mathbb{Z}, x \not\equiv 0 \mod n \Rightarrow x \not\equiv -x,\ \mathbb{Z}_n = \{0, x_1, -x_1, .., x_{\frac{n-1}{2}}, -x_{\frac{n-1}{2}}\}$
- $p \in \mathbb{P}, p > 2 \Rightarrow \{1, .., \frac{p-1}{2}\}$ Halbsystem
- $n \in 2\mathbb{N}+1,\ y \in \mathbb{Z}_n^*,\ H, \widetilde{H}$ Halbsysteme $\Rightarrow \prod_{x\in H} \varepsilon_x(y) = \prod_{x\in\widetilde{H}} \widetilde{\varepsilon}_x(y)$
- $\chi_n : \mathbb{Z}_n^* \to \{-1, 1\}$ Homomorphismus
- $p \in \mathbb{P}\backslash\{2\},\ x \in \mathbb{Z}_p^*$: $\chi_p(x) = 1 \Leftrightarrow x$ Quadrat in $\mathbb{Z}_p^*$
- $m \equiv m' \mod n \Rightarrow (\frac{m}{n}) = (\frac{m'}{n})$
- $m_1, m_2 \in \mathbb{Z},\ n \in 2\mathbb{N}+1$: $(\frac{m_1 m_2}{n}) = (\frac{m_1}{n}) \cdot (\frac{m_2}{n})$
- $m \in \mathbb{Z}, n \in 2\mathbb{Z}+1$: $(m,n) = 1 \Rightarrow (\frac{m}{n}) = \prod_{k=1}^{\frac{n-1}{2}} \operatorname{sgn}\big(R(\frac{km}{n})\big)$
- Lemma von Kronecker:
  $m \in 2\mathbb{N}+1,\ 0 < x < \frac{1}{2} \Rightarrow \operatorname{sgn}\big(R(xm)\big) = \prod_{h=1}^{\frac{m-1}{2}} \operatorname{sgn}\big((x-\frac{h}{m})(x+\frac{h}{m}-\frac{1}{2})\big)$
- **Quadratisches Reziprozitätsgesetz**: $n, m \in \mathbb{N}\backslash\{1\} \Rightarrow (\frac{n}{m}) = (-1)^{\frac{1}{4}(n-1)(m-1)} (\frac{m}{n})$
- **Ergänzungssätze vum Reziprozitätsgesetz**:
  $n \in 2\mathbb{N}+1 \Rightarrow (\frac{-1}{n}) = (-1)^{\frac{n-1}{2}},\ (\frac{2}{n}) = (-1)^{\frac{1}{8}(n^2-1)} = \begin{cases} 1 & n \equiv \pm 1 \mod 8 \\ -1 & n \equiv \pm 3 \mod 8 \end{cases}$
- $m \in \mathbb{Z},\ n_1, n_2 \in 2\mathbb{N}+1 \Rightarrow (\frac{m}{n_1 n_2}) = (\frac{m}{n_1}) \cdot (\frac{m}{n_2})$

- $n, c \in \mathbb{Z}, n \geq 2, c+n\mathbb{Z} \in \mathbb{Z}_n^*$:
  - n ungerade: $c+n\mathbb{Z}$ Quadrat in $\mathbb{Z}_n^* \Leftrightarrow (\frac{c}{p}) = 1\ \forall p \in \{q \in \mathbb{P} :\ q \neq 2,\ , q | n\}$
  - $2|n, 4 \not| n$: $c+n\mathbb{Z}$ Quadrat in $\mathbb{Z}_n^* \Leftrightarrow (\frac{c}{p}) = 1\ \forall p \in \{q \in \mathbb{P} :\ q \neq 2,\ , q | n\}$
  - $4|n, 8 \not| n$: $c+n\mathbb{Z}$ Quadrat in $\mathbb{Z}_n^* \Leftrightarrow (\frac{c}{p}) = 1\ \forall p \in \{q \in \mathbb{P} :\ q \neq 2,\ , q | n\},\ c \equiv 1 \mod 4$
  - $8|n$: $c+n\mathbb{Z}$ Quadrat in $\mathbb{Z}_n^* \Leftrightarrow (\frac{c}{p}) = 1\ \forall p \in \{q \in \mathbb{P} :\ q \neq 2,\ , q | n\},\ c \equiv 1 \mod 8$

4.3 Primzahlen mit vorgegebenen Restklassen

- $|\{p \in \mathbb{P} :\ p \equiv -1 \mod 3\}| = \infty$
- $|\{p \in \mathbb{P} :\ p \equiv -1 \mod 4\}| = \infty$
- $|\{p \in \mathbb{P} :\ p \equiv 1 \mod 4\}| = \infty$
- $0 \neq a \in \mathbb{Z} \Rightarrow |\{p \in \mathbb{P} :\ (\frac{a}{p}) = 1\}| = \infty$
- $|\{p \in \mathbb{P} :\ p \equiv 1 \mod 3\}| = \infty$
- $a \in \mathbb{Z}, a \neq b^2\ \forall b \in \mathbb{Z} \Rightarrow |\{p \in \mathbb{P} :\ (\frac{a}{p}) = -1\}| = \infty$

4.4 Darstellung von Primzahlen als Quadratsummen

- **Lemma von Thue**: $p \in \mathbb{P}, e, f \in \mathbb{N}\backslash\{1\}, e\cdot f > p, r \in \mathbb{Z} \Rightarrow \exists x, y \in \mathbb{Z} :\ (ry \equiv x \mod p \vee ry \equiv -x \mod p) \wedge (0 \leq x < e \wedge 1 \leq y < f)$
- **Satz von Lagrange**: $p \in \mathbb{P}\backslash\{2\} :\ \exists x, y \in \mathbb{N} :\ p = x^2 + y^2 \Leftrightarrow p \equiv 1 \mod 4$
- $p \in \mathbb{P}\backslash\{2,3\} :\ \exists x, y \in \mathbb{N} :\ p = x^2 + 3y^3 \Leftrightarrow p \equiv 1 \mod 3$

5 Diophantische Gleichungen

Eine **diophantische Gleichung** ist eine Gleichung $f(x_1, .., x_k) = 0$ zusammen mit der Frage nach ganzzahligen Lösungen $(x_1, .., x_k) :\ x_i \in A_i \subset \mathbb{Z}$

Beispiel: **Pythagoras**

$$x^2 + y^2 - z^2 = 0$$

Lösung nach Pythagoras: $x = m,\ y = \frac{1}{2}(m^2-1)\ z = \frac{1}{2}(m^2+1)$
Es gibt weitere Lösungen, etwa (8,5,17) $\big((n+2)^2 - n^2 = 4n+4\big)$

5.1 Lineare diophantische Gleichnugen

$$\sum_{i=1}^{k} a_i x_i = n, \quad a_1, .., a_k, x_1, .., x_k, n \in \mathbb{Z}$$

- $\sum_{i=1}^{k} a_i x_i = n$ lösbar, $a_1, .., a_k, x_1, .., x_k, n \in \mathbb{Z} \Leftrightarrow (a_1, .., a_k) | n$

- $c_1,..,c_s,a \in \mathbb{Z}:\ \big([c_1,a],..,[c_s,a]\big) = \big[(c_1,..,c_s),a\big]$
- $a_1,..,a_k \in \mathbb{N},\ n \in \mathbb{Z},\ \sum_{i=1}^k a_i x_i = n$ Diophantische Gleichung
  - $d_i := (a_1,..,a_i), b_i := \frac{d_{i-1}}{d_i},\ \sum_{i=1}^k a_i x_i = n$ lösbar $\Rightarrow\ \exists! x_1,..,x_k:\ 0 \le x_i < b_i\ \forall i = 2,..,k$
  - $d_{i,j} := (d_i,a_j); \forall i<j, b_{i,j} := \frac{d_{i-1,j}}{d_{i,j}}, x_1,..,x_k,\ y_1,..,y_k$ Lösungen $\Rightarrow\ \exists!(t_{i,j}) \in \mathbb{Z}^{k\times k}$:
    1. $y_i = x_i + \sum_{j=1}^k t_{i,j}\frac{a_j}{(a_i,a_j)}$
    2. $t_{i,j} = -t_{j,i} \quad \forall i,j \quad (\Rightarrow\ t_i i = 0)$
    3. $0 \le t_{i,j} < \frac{b_i}{b_{i,j}} \quad \forall\ 2 \le i < j \le k$
- $a_1,..,a_k,n \in \mathbb{N}:\ (a_1,..,a_n) = 1,\ b_i := \frac{(a_1,..,a_{i-1})}{(a_1,..,a_i)}, \forall\ 2 \le i \le k:$
  $n \ge \sum_{i=2}^k (b_i - 1)a_i - a_1 + 1 \Rightarrow\ \exists y_1,..,y_k \in \mathbb{N}:\ \sum_{i=1}^k a_i y_i = n$
- $n = a_1x_1 + a_2x_2,\ a_1,a_2 \in \mathbb{N}, d := (a_1,a_2),\ a_1y_1 + a_2y_2 = n, y_1,y_2 \in \mathbb{Z}:$
  $\exists\ z_1,z_2 \in \mathbb{N}:\ a_1z_1 + a_2z_2 = n \Leftrightarrow\ e := \lfloor\frac{y_1 d}{a_2}\rfloor + \lfloor\frac{y_2 d}{a_1}\rfloor \ge 0 \quad \Rightarrow \exists$ genau $e+1$ verschiedene Lösungen $z_1,z_2 \in \mathbb{N}_0$

5.2 Hindernisse

In bestimmten Fällen kann man sofort ausschließen, dass eine diophantische Gleichung eine Lösung hat.

1. Hat eine Gleichung keine reelle Lösung, so auch keine ganzzahlige Lösung. Zum Beispiel: $x^2 + xy + y^2 + 1 = 0$, da $x^2 + y^2 - xy \ge 0\ y]\forall x,y \in \mathbb{R}$
2. Mit dem Zwischenwertsatz kann man abschätzen, wo Lösungen liegen. Liegen sie zwischen zwei aufeinanderfolgenden Zahlen, so kann es keine ganzzahlige Lösung geben. Zum Beispiel:
   $f(x) := 3x^3 + 5x^2 - 1, \quad f(-2) < 0 < f(-1),\ f(0) < 0 < f(1)$
3. Hat eine Gleichung $\mod n$ keine Lösung, so hat sie auch keine ganzzahlige Lösung. Die Modulorechnung vereinfacht viele Aufgaben. Zum Beispiel:
   $x^2 - y^2 \equiv 2 \mod 4$ hat keine Lösung $\Rightarrow\ x^2 + 3y^2 - 23242 = 0$ hat keine Lösung in $\mathbb{Z}$

Zu 3.: Die Umkehrung gilt allerdings nicht! Etwa: $x^4 - 2y^2$ hat keine rationalen Lösungen, $x^4 - 2y^2 \equiv 17 \mod n$ besitzt aber $\forall n \ge 2$ eine Lösung (Reinhardt).

5.3 Pell'sche Gleichungen

Definitionen

- **Pell'sche Gleichung**: Diophantische Gleichung $x^2 - Dy^2 = 1$ mit $D \in \mathbb{Z}$
- $u + v\sqrt{D}$ **Pell'sche Einheit** $:\Leftrightarrow\ (u,v)$ löst die Pell'sche Gleichung

Sätze

- **Dirichlet'scher Approximationssatz:**
  $\alpha \in \mathbb{R}, t \in \mathbb{N} \Rightarrow\ \exists x,y \in \mathbb{Z}:\ 1 \le y \le t,\ |\alpha y - x| \le \frac{1}{t+1}$
- $\alpha \in \mathbb{R}\backslash\mathbb{Q} \Rightarrow\ \big|\{(x,y) \in \mathbb{Z}^2:\ (x,y) = 1, |x - \alpha y| < \frac{1}{y}\}\big| = \infty$
- $D \in \mathbb{N}$ kein Quadrat $\Rightarrow\ \big|\{(x,y) \in \mathbb{N}:\ (x,y) = 1, |x^2 - Dy^2| < 1 + 2\sqrt{D}\}\big| = \infty$
- $D \in \mathbb{N}$ kein Quadrat $\Rightarrow\ \exists (x,y) \in \mathbb{N}, y \ne 0:\ x^2 - Dy^2 = 1$

5.4 Link zur Algebra

Betrachte den Ring $\mathbb{Z}(\sqrt{D})$:

- $D \in \{0,1\} \Rightarrow\ \mathbb{Z}(\sqrt{D}) = \mathbb{Z}$
- $D = n^2D' \Rightarrow\ \mathbb{Z}(\sqrt{D}) = \mathbb{Z}(\sqrt{D'})$
- $Q\big(\mathbb{Z}(\sqrt{D})\big) = \mathbb{Q}(\sqrt{D})$
- $Aut_{\mathbb{Q}(\sqrt{D})} = \{\mathrm{id}, \bar{}\}, \quad \overline{a + b\sqrt{D}} = a - b\sqrt{D}$

Im Folgenden sei $D \notin \{0,1\}$ quadratfrei.

Definitionen

- $w \in \mathbb{Z}(\sqrt{D})$: **Norm** $N(w) : \mathbb{Z}(\sqrt{D}) \to \mathbb{Z},\ w \mapsto w \cdot \overline{w}$
- $a,b \in \{x,y \in \mathbb{N}^2:\ x^2 - Dy^2 = 1\}$ **Minimallösung** $:\Leftrightarrow\ b$ minimal

Sätze

- w Einheit von $\mathbb{Z}(\sqrt{D}) \Leftrightarrow\ w \in \mathbb{Z}(\sqrt{D}):\ |N(w)| = 1$
- $C \in \mathbb{N}$ quadratfrei $\Rightarrow\ \big|\{(x,y) \in \mathbb{Z}^2:\ x^2 - Cy^2 = 1\}\big| = \infty$
- a,b Minimallösung von $x^2 - Dy^2 = 1, w := a + b\sqrt{D} \Rightarrow\ x = \frac{w^n + \overline{w}^n}{2},\ y = \frac{w^n - \overline{w}^n}{2\sqrt{D}},\ n \in \mathbb{N}$ alle Lösung $x,y > 0$ von $x^2 - Dy^2 = 1$
- a,b Lösung von $x^2 - Dy^2 = 1,\ s,t$ Lösung von $x^2 - Dy^2 = g \Rightarrow\ (a + b\sqrt{D})^n(s + t - \sqrt{D}) = u + v\sqrt{D},\ n \in \mathbb{N}$ liefert Lösung u,v von $x^2 - Dy^2 = g$

5.5 Allgemeine quadratische Gleichungen

$$0 = f(x,y) = c_{00} + 2c_{01}x + 2c_{02}y + c_{11}x^2 + c_{22}y^2 + 2c_{12}xy$$

$$\Leftrightarrow\ \begin{pmatrix}1 & x & y\end{pmatrix} C \begin{pmatrix}1\\x\\y\end{pmatrix} = 0,\ c_{ji} := c_{ij} \quad \textbf{allgemeinequadratischeGleichung}$$

Im Folgenden sei $\det(C) \ne 0$.

Mit $d := c_{12}^2 - c_{11}c_{22},\ l := c_{01}c_{22} - c_{02}c_{11},\ m := c_{02}c_{11} - c_{01}c_{12}$ unterscheidet man dan die folgenden Fälle:

1. $d = 0$
   $\Rightarrow\ c_{11} \neq 0\ \vee\ c_{22} \neq 0$ (da $\det C \neq 0$), o.E. $c_{11} \neq 0$
   $\Rightarrow\ \exists r, s \in \mathbb{Z}:\ f(x,y) = 0 \Leftrightarrow\ (c_{01} + c_{11}x + c_{12}y)^2 = r + sy$
   $r \mod s$ kein Quadrat $\Rightarrow$ nicht lösbar
   $r \mod s$ Quadrat, $z^2 \equiv r \mod s \Rightarrow$ Löse $c_{01} + c_{11}x + c_{12}y = z$
   lösbar, falls $c_{11} | (z - c_{01} - c_{12}y)$
   Falls z diese Eigenschaft erfüllt, so auch z' mit $c_{11}s | z'$

2. $d \neq 0, c_{11} = c_{22} = 0$
   $f(x,y) = 0\ \Leftrightarrow\ 2(dx - l)(dy - m) = c_{23}\det(C)$
   Es gibt nur endlich viele Lösungen.

3. $d \neq 0, c_{11} \neq 0$
   $f(x,y) = 0\ \Leftrightarrow\ (dy - m)^2 - d(c_{01} + c_{11}x + c_{12}y)^2 = -c_{11}\det(C)$
   Löse also $u^2 - dv^2 = g := -c_{11}\det(C)$ mit Hilfsproblem $x^2 - dy^2 = 1$
   Löse $u = dy - m,\ v = c_{01} + c_{11}x + c_{12}y$

Satz:
Sei $\det(C) \neq 0$ und d kein Quadrat. Dann gilt:

$$f(x,y) = 0 \quad \Leftrightarrow \quad (dy - m)^2 - d(c_{01} + c_{11}x + c_{12}y)^2 = -c_{11}\det(C)$$

und es lassen sich unendlich viele Lösungen konstruieren.

6 Entwicklung reeller Zahlen

6.1 Die g-adische Entwicklung

Im Folgenden sei $g \in \mathbb{N}\backslash\{2\}$.

Definitionen

- $a_k..a_1a_0$ **g-adische Darstellung** von $n \in \mathbb{N}_0 :\Leftrightarrow k = \lfloor \log_g n \rfloor,\ n = \sum_{i=0}^{k} a_i g^i,\ a_i \in \{0,..,g-1\}$
- $\sum_{i=0}^{k} a_i,\ k = \lfloor \log_g n \rfloor$ **g-adische Quersumme von** n
- $\sum_{i=0}^{k} (-1)^i a_i,\ k = \lfloor \log_g n \rfloor$ **alternierende g-adische Quersumme von** n
- $r = \sum_{i \geq -k} a_i g^{-i},\ a_i \in \{0,..,g-1\}$ **g-adische Darstellung von r** $\in \mathbb{R}$
- $r = \sum_{i \geq 1} a_i g^{-i}$ periodisch, $p \in \mathbb{N}$ minimal mit der Eigenschaft : $\exists l \in \mathbb{N}_0:\ a_i = a_{i+p}\ \forall i \geq l+1,\ l$ minimal
  - p **Periodenlänge**, l **Vorperiodenlänge**
  - $l = 0$: r **reinperiodisch**
  - $l > 0$: r **gemischperiodisch**

Sätze

- $n \in \mathbb{N}_0 \Rightarrow\ \exists! a_i \in \{0,1,..,g-1\}:\ n = \sum_{i \geq 0} a_i g^i$
- Sei $n = \sum_{i=0}^{k} a_i g^i$ mit $a_i \in \{0,..,g-1\}$.
  - $d | g \Rightarrow\quad [d|n \Leftrightarrow\ d|a_0]$
  - $d | (g-1) \Rightarrow\quad [d|n \Leftrightarrow\ d | \sum_{i=0}^{k} a_i]$
  - $d | (g+1) \Rightarrow\quad [d|n \Leftrightarrow\ d | \sum_{i=0}^{k} (-1)^i a_i]$
- Sei $n = \sum_{i=0}^{k} a_i g^i$ mit $a_i \in \{0,..,g-1\}$.
  - $d | (g^2-1) \Rightarrow\ d | g^{2i} - 1\ \forall i \in \mathbb{N}$
  - $d | (g^2-1) \Rightarrow\ n \equiv (a_0 + a_1 g) + (a_2 + a_3 g) + ..\mod d$
  - $d | (g^2+1) \Rightarrow\ g^{2i} \equiv (-1)^i \mod d$
  - $d | (g^2+1) \Rightarrow\ n \equiv (a_0 + a_1 g) - (a_2 + a_3 g) \pm ... \mod d$
  - $d | (g^s \pm 1) \Rightarrow\ [d|n \Leftrightarrow\ d$ teilt die (bei $-$ alternierende) "Quersumme" von n in Päckchen der Länge $s]$
- $g \in \mathbb{N}\backslash\{1\},\ r \in \mathbb{R}:\ 0 < r < 1 \Rightarrow\ \exists!\ \sum_{i \geq 1} a_i g^{-i} = r,\ a_i \in \{0,1,..,g-1\},\ |\{a_i :\ a_i \neq g-1\}| = \infty$
- $g \in \mathbb{N}\backslash\{1\},\ 0 < r = \sum_{i \geq 1} a_i g^{-1} < 1:\ r \in \mathbb{Q} \Leftrightarrow\ \exists\, l, p \in \mathbb{N}:\ a_i = a_{i+p}\ \forall i \geq l+1$
- $r = \frac{a}{b},\ (a,b) = 1,\ b = b^* \cdot b',\ b^*$ größter Teiler von b, der teilerfremd zu g ist $\Rightarrow\ p =$ Ordnung von g in $\mathbb{Z}_{b^*}^* =$ kleinste Zahl s mit $b^* | g^s - 1$, $l =$ kleiste Zahl s mit $b' | g^s$

6.2 Kettenbruchdarstellung

Definitionen

- $a_0,..,a_n \in \mathbb{R},\ a_i \geq 1\ \forall i \geq 1:\ [a_0] := a_0,\ [a_0; a_1,..,a_n] := a_0 + \frac{1}{[a_1; a_2,..,a_n]}$
- $[a_0; a_1,..,a_n]$ **endlicher Kettenbruch** $:\Leftrightarrow\ a_0 \in \mathbb{Z},\ a_i \in \mathbb{N}\ \forall i \geq 1$
- $a_0 \in \mathbb{Z}, (a_j)_{j \in \mathbb{N}} \subset \mathbb{N}:\ A_i := [a_0; a_1,..,a_i]$ **i-ter Näherungsbruch von** $[a_0; a_1, a_2, ..]$
- $r = [a_0; a_1, a_2, ..]$ **unendlicher Kettenbruch** $:\Leftrightarrow\ A_i \xrightarrow{i \to \infty} r$

Sätze

- $a_0 \in \mathbb{Z}, a_i \in \mathbb{N}\ \forall i \in \mathbb{N} \Rightarrow\ [a_0; a_1,..,a_n] \in \mathbb{Q}$
- $q \in \mathbb{Q} \Rightarrow\ \exists!\, [a_0; a_1,..,a_n] = q:\ [n \geq 1 \Rightarrow\ a_n > 1]$
- Seien für $i \geq 0\ p_i, q_i \in \mathbb{Z}:\ q \geq 1,\ (p_i, q_i) = 1,\ [a_0; a_1,..,a_i] = \frac{p_i}{q_i}$ und setze $p_{-1} := 1,\ q_{-1} := 0$. Dann gilt für $i \geq 1$:
  - $p_i = a_i p_{i-1} + p_{i-2},\quad q_i = a_i q_{i-1} + q_{i-2}$
  - $r \in \mathbb{R}^+ \Rightarrow\ [a_0; a_1,..,a_{i-1}, r] = \frac{r p_{i-1} + p_{i-2}}{r q_{i-1} + q_{i-2}}$

  - $p_{i-1}q_i - p_iq_{i-1} = (-1)^i$

- $(a_i)_i$ Folge, $A_i = [a_0; a_1, .., a_i]$
  - $a_i \geq i$
  - $A_{i-1} - A_i = \frac{(-1)^i}{q_iq_{i-1}}, \quad A_i - A_{i-2} = \frac{(-1)^i a_i}{q_iq_{i-2}}$
  - $A_0 < A_2 < A_4 < .., \quad .. < A_5 < A_3 < A_1$
  - $A_i \xrightarrow{i\to\infty} s \in \mathbb{R}\backslash\mathbb{Q}$
- $r \in \mathbb{R}\backslash\mathbb{Q} \Rightarrow \exists! \, [a_0; a_1, a_2, ..] = r$