Vorlesung Analytische Zahlentheorie

SoSe'22, hhu
K. Halupczok

AnZ 2: Grundlagen über zahlentheoretische Funktionen

Stichworte: zahlentheoretische Funktion (zth. Fkt.), Faltungsprodukt $*$, Liste zth. Fktn., (vollständig) multiplikative/additive zth. Fktn., Möbiusfunktion μ, Formel $\mu * \mathbb{1} = \varepsilon$, Möbiussche Umkehrformeln, Faltungsidentitäten, sprunghaftes Verhalten von τ, Mittelwerte

---

2.1. Einleitung: Zahlentheoretische Funktionen (auch: "arithmetische Funktionen") sind komplexwertige Folgen, die einen Bezug zu zahlentheoretischen Fragestellungen haben.

2.2. Def.: • zahlentheoretische Funktion: Funktion $f: \mathbb{N} \to \mathbb{C}$ bzw. komplexwertige Folge (f_n)

• (Ihre erzeugende Dirichletreihe ist $\sum_{n \geq 1} f(n) n^{-s}$ für $s \in \mathbb{C}$.)

• Schreiben auch a_n für $a(n)$, wenn $a: \mathbb{N} \to \mathbb{C}$ eine zth. Fkt. ist.
$\hat{=}$ Abkürzung

• Faltungsprodukt/Dirichlet-Produkt zweier zth. Fktn. a und b ist $a * b = c$

mit $c_n := \sum_{d \mid n} a_d b_{n/d} = \sum_{d \mid n} a(d) b(\frac{n}{d}) = \sum_{\substack{d,t \\ dt = n}} a(d) b(t)$ ← t ist "Gegenteiler" von d

2.3. Satz: • Die zth. Fktn. bilden mit $*$ eine abelsche Halbgruppe mit neutralem Element ε,

wo $\varepsilon(n) = \lfloor \frac{1}{n} \rfloor = \begin{cases} 1, & n = 1 \\ 0, & n \neq 1 \end{cases}$ die "1-Erkennungsfkt." ist.
$\hat{=}$ Gaußklammer: $\lfloor x \rfloor = \max\{ n \in \mathbb{Z};\ n \leq x \}$

• Die zth. Fktn. f mit $f(1) \neq 0$ bilden mit $*$ eine abelsche Gruppe.

Beweisskizze: • Die Kommutativität und Assoziativität von $*$ ist leicht nachzurechnen.

• Mit $f(1) \neq 0 \neq g(1)$ folgt auch $f * g(1) = \sum_{d \mid 1} f(d) g(\frac{1}{d}) = f(1) g(1) \neq 0$. • Weiter ist $f * \varepsilon(n) = \sum_{d \mid n} f(d) \cdot \underbrace{\varepsilon(\tfrac{n}{d})}_{\Rightarrow d = n} = f(n)$.

• Zum Nachweis eines Inversen g von f mit $f(1) \neq 0$ wird die Glg. $g * f \overset{!}{=} \varepsilon$ rekursiv nach g aufgelöst: Rekursionsanf.: $g(1) \cdot f(1) \overset{!}{=} 1$ ergibt $g(1) := \frac{1}{f(1)}$, ok, da $f(1) \neq 0$.

Rekursionsschritt: Ist $g(m)$ für alle $m \leq n$ berechnet, folgt, dass

$$(g * f)(n+1) \overset{!}{=} \varepsilon(n+1) = 0 \iff 0 \overset{!}{=} g(n+1) f(1) + \sum_{\substack{d \mid n+1 \\ d \neq n+1}} g(d) f\left(\frac{n+1}{d}\right) \text{ erfüllt ist,}$$

wenn $g(n+1) := -\frac{1}{f(1)} \cdot \sum_{d \mid n+1,\, d \neq n+1} g(d) f\left(\frac{n+1}{d}\right)$ gesetzt wird. $\square$

2.4. Liste wichtiger zahlentheoretischer Funktionen (zth. Fktn.):

- konstant-1-Fkt.: $\mathbb{1}(n) := 1$ für alle $n \in \mathbb{N}$ •Identität: $id(n) := n$
- 1-Erkennungsfkt.: $\varepsilon(n) := \lfloor \frac{1}{n} \rfloor = \begin{cases} 1, & n=1 \\ 0, & n>1 \end{cases}$
- Möbiusfkt.: $\mu(n) := \begin{cases} 1, & n=1 \\ 0, & \exists p : p^2 \mid n \\ (-1)^k, & \text{sonst} : n = p_1 \cdots p_k \end{cases}$

- Teileranzahlfkt.: $\tau(n) := \#\{t \mid n\} = \sum_{ts=n} 1$, auch: $d(n)$ genannt
- verallg. Teileranzahlfkt.: $\tau_k(n) := \sum_{t_1 \cdots t_k = n} 1$ = Anz. Möglichkeiten, n als Produkt aus k vielen Faktoren $\in \mathbb{N}$ zu schreiben (auch: Dirichlet-Piltz-Teilerfkt. genannt)
- Teilersummenfunktion: $\sigma(n) := \sum_{t \mid n} t$
- Dirichlet-Charakter: $\chi(n)$ zum Modul q
- Potenzteilersummenfunktion zum Exponenten $\alpha \in \mathbb{R}$: $\sigma_\alpha(n) := \sum_{t \mid n} t^\alpha$
- Potenzfkt.: $P_\alpha(n) := n^\alpha$
- Eulersche φ-Funktion: $\varphi(n) := \#\{a \in \{1, \dots, n\};\ ggT(a,n) = 1\} = \sum_{\substack{1 \le a \le n \\ (a,n)=1}} 1$
- von Mangoldt-Fkt.: $\Lambda(n) := \begin{cases} \log p, & n = p^k \text{ für ein } k \in \mathbb{N}, p \in \mathbb{P} \\ 0, & \text{sonst} \end{cases}$
- Ramanujan-Summe: $c_q(n) = \sum_{\substack{a \le q \\ (a,q)=1}} e^{2\pi i a n / q}$
- Anz. Darstellungen als Summe zweier □e: $R_{2,2}(n) := \#\{(a,b) \in \mathbb{N}^2;\ n = a^2 + b^2\}$
- Anz. Darstellungen als Summe l vieler k-ten Potenzen: $R_{k,l}(n) := \#\{(a_1, \dots, a_l) \in \mathbb{N}^l;\ n = \sum_{i=1}^{l} a_i^k\}$

- Primteileranzahlfkt.: $\omega(n) := \#\{p \in \mathbb{P};\ p \mid n\} = \sum_{p \mid n} 1$
- Primfaktorenanzahlfkt.: $\Omega(n) := \#\{(p,j) \in \mathbb{P} \times \mathbb{N};\ p^j \mid n\} = \sum_p \sum_{\substack{j \ge 1 \\ p^j \mid n}} 1$

  Ist $n = p_1^{a_1} \cdots p_r^{a_r}$ die PFZ von n, ist $\omega(n) = r$
  und $\Omega(n) = a_1 + \ldots + a_r$.

  Ist $\underbrace{p^{e(p)} \| n}_{\text{d.h. } p^{e(p)} \mid n,\ p^{e(p)+1} \nmid n}$, gilt also $\Omega(n) = \sum_p e(p)$. ⇝ Schreibe: $\Omega(n) = \sum_{p^k \| n} k$.

2.5. **Bem.:** Bei den Definitionen von ω und Ω wird der Unterschied zwischen Prim<u>teiler</u> / Prim<u>faktor</u> deutlich: beidesmal ist zwar eine Primzahl p mit $p \mid n$ gemeint. Aber in ihrer <u>Primfaktorzerlegung</u> (kurz: PFZ, laut Satz von der eindeutigen PFZ in $\mathbb{N}$ = Fundamentalsatz der Arithmetik) wird bei Zählung der Prim<u>faktoren</u> die Vielfachheit berücksichtigt, bei Prim<u>teilern</u> nicht.

2.6. In der folgenden Def. bezeichnet (m,n) den ggT von m,n. Die Kurzschreibweise wird in der Zahlentheorie bevorzugt, da der ggT so häufig vorkommt und die Notation $ggT(m,n)$ oder $gcd(m,n)$ schnell lästig wird. Meist ist keine Kollision mit anderen Notationen zu befürchten. Erinnerung:

- $d \in \mathbb{N}$ heißt ggT von m und n, falls $t|m \wedge t|n \Rightarrow t|d$ gilt.
- $m,n \in \mathbb{N}$ heißen teilerfremd, falls $(m,n)=1$ ist.

2.7. Def.: Eine zth. Fkt. $f: \mathbb{N} \to \mathbb{C}$ heißt

- multiplikativ, falls $\forall m,n \in \mathbb{N}, (m,n)=1: f(mn)=f(m)\cdot f(n)$
- vollständig multiplikativ, falls $\forall m,n \in \mathbb{N}: f(mn)=f(m)\cdot f(n)$
- additiv, falls $\forall m,n \in \mathbb{N}, (m,n)=1: f(mn)=f(m)+f(n)$
- vollständig additiv, falls $\forall m,n \in \mathbb{N}: f(mn)=f(m)+f(n)$

Klar sind vollständig multiplikative/additive zth. Fktn. auch multiplikativ/additiv.

2.8. Bem.: Die zth. Fktn. der Liste 2.4 haben folgende Eigenschaften:

- vollständig multiplikativ: $\mathbb{1}, \varepsilon, P_\alpha$
- multiplikativ, nicht vollst. mult.: $\mu, \tau, \tau_k, \sigma, \sigma_\alpha, \varphi, R_{e,k}$
- vollständig additiv: Ω
- additiv, nicht vollst. add.: ω

Die multiplikativen zth. Fktn. sind aus zahlentheoretischer Sicht besonders interessant, da die Eigenschaft "multiplikativ" beim Faltungsprodukt erhalten bleibt:

2.9. Satz: Die Menge der multiplikativen zth. Fktn. bildet mit $*$ eine Untergruppe der abelschen Gruppe der zth. Fktn. f mit $f(1) \neq 0$.

Beweis: Die Abgeschlossenheit bzgl. $*$ ist zu zeigen. Seien f,g mult. zth. Fktn. und $(m,n)=1$. Die Teiler $d|mn$ sind dann eineindeutig schreibbar als $d=d_1d_2$ mit $d_1|m, d_2|n$, wobei dann auch $(d_1,d_2)=\left(\frac{m}{d_1},\frac{n}{d_2}\right)=1$ gelten. Es folgt

$$(f*g)(mn)=\sum_{d|mn} f(d)g\left(\frac{mn}{d}\right)=\sum_{d_1|m,\, d_2|n} f(d_1d_2)g\left(\frac{mn}{d_1d_2}\right)\underset{f,g \text{ mult.}}{=}\sum_{\substack{d_1|m\\ d_2|n}} f(d_1)f(d_2)\,g\left(\frac{m}{d_1}\right)g\left(\frac{n}{d_2}\right)$$

$$=\sum_{d_1|m} f(d_1)g\left(\frac{m}{d_1}\right)\sum_{d_2|n} f(d_2)g\left(\frac{n}{d_2}\right)=(f*g)(m)\cdot(f*g)(n). \qquad \square$$

Speziell die Möbiusfunktion spielt eine zentrale Rolle:

2.10. **Satz:** • Die Möbiusfunktion $\mu(n)=\begin{cases}(-1)^r, & n=p_1\cdots p_r \text{ mit p.w.v. } p_1,\dots,p_r \text{ prim},\\ 1, & n=1\\ 0, & \text{sonst, d.h. } \exists p \text{ prim}: p^2 \mid n\end{cases}$ ist multiplikativ.

• μ ist Faltungsinverse der Fkt. $\mathbb{1}(n)=1$, d.h. $\mu*\mathbb{1}=\varepsilon$.
die Konstant-1-Fkt.: $\mathbb{1}(n):=1$ für alle $n\geq 1$

Bew.: • Es ist μ multiplikativ: $\mu(mn)=\mu(m)\mu(n)$ stimmt für "quadrathaltige" teilerfremde m,n, und mit $(m,n)=1$, $m=p_1\cdots p_r$, $n=\tilde{p}_1\cdots\tilde{p}_s$ folgt $\mu(mn)=(-1)^{r+s}=\mu(m)\mu(n)$, auch falls $m=1$ oder $n=1$.
• Mit μ und $\mathbb{1}$ ist dann auch $\mu*\mathbb{1}$ multiplikativ (nach Satz 2.9).
• Es genügt dann, die Faltungsformel $\mu*\mathbb{1}(n)=\varepsilon(n)$ auf Primpotenzen $n=p^k$ (und $n=1$) nachzuweisen, denn mit der PFZ $n=p_1^{k_1}\cdots p_r^{k_r}$ folgt dann $\mu*\mathbb{1}(p_1^{k_1}\cdots p_r^{k_r})=(\mu*\mathbb{1})(p_1^{k_1})\cdots(\mu*\mathbb{1})(p_r^{k_r})=\varepsilon(p_1^{k_1})\cdots\varepsilon(p_r^{k_r})=\varepsilon(p_1^{k_1}\cdots p_r^{k_r})$, also $\mu*\mathbb{1}=\varepsilon$.
• Dazu sei p^k eine beliebige Primpotenz. Dann ist

$$\mu*\mathbb{1}(p^k)=\sum_{d\mid p^k}\mu(d)=\mu(1)+\mu(p)+\mu(p^2)+\dots+\mu(p^k)=1+(-1)+0+\dots+0=0=\varepsilon(p^k),$$

sowie $\mu*\mathbb{1}(1)=\sum_{d\mid 1}\mu(d)\mathbb{1}(\frac{1}{d})=\mu(1)\mathbb{1}(1)=1\cdot 1=1$. □

Die Faltungsformel $\boxed{\mu*\mathbb{1}=\varepsilon}$ kann bereits als Möbiussche Umkehrformel bezeichnet werden. Üblicherweise bezeichnet man damit aber folgenden Satz:

2.11. Möbiussche Umkehrformeln: 1) Für zth. Fkn. f und g sind äquivalent:
(i) $g(n)=\sum_{d\mid n}f(d)$ für alle $n\in\mathbb{N}$, (ii) $f(n)=\sum_{d\mid n}\mu(d)g(\frac{n}{d})$ für alle $n\in\mathbb{N}$.
2) Für $F,G:[1,\infty)\to\mathbb{C}$ sind äqu.: (i) $F(x)=\sum_{n\leq x}G(\frac{x}{n})$ für $x\geq 1$, (ii) $G(x)=\sum_{n\leq x}\mu(n)F(\frac{x}{n})$ für $x\geq 1$.

Bew.: Zu 1.): $\forall n: g(n)=\sum_{d\mid n}f(d) \iff g=f*\mathbb{1} \overset{*\mu}{\iff} \mu*g=f*\underbrace{\mathbb{1}*\mu}_{=\varepsilon}$
$\iff f=\mu*g \iff \forall n: f(n)=\sum_{d\mid n}\mu(d)g(\frac{n}{d})$.

Zu 2.): Diese Variante kann manchmal nützlich sein. Es ist für $x\geq 1$:

"$\Rightarrow$": $\sum_{n\leq x}\mu(n)F(\frac{x}{n})=\sum_{n\leq x}\mu(n)\sum_{m\leq x/n}G(\frac{x}{mn})\overset{mn=:k}{=}\sum_{k\leq x}G(\frac{x}{k})\underbrace{\sum_{n\mid k}\mu(n)}_{=\varepsilon(k)}=G(\frac{x}{1})=G(x)$.

"$\Leftarrow$": $\sum_{n\leq x}G(\frac{x}{n})=\sum_{n\leq x}\sum_{m\leq x/n}\mu(m)F(\frac{x}{mn})\overset{"}{=}\sum_{k\leq x}F(\frac{x}{k})\underbrace{\sum_{m\mid k}\mu(m)}_{=\varepsilon(k)}=F(\frac{x}{1})=F(x)$. □

Neben der fundamentalen Faltungsidentität $\mu * \mathbb{1} = \varepsilon$ gibt es noch weitere, die interessant sind:

2.12. <u>Faltungsidentitäten:</u>
(bei multipl. zth. Fktn. genügt es, die Übereinstimmung auf Primpotenzen (und 1) zu testen)

$$\boxed{\begin{array}{ll} \mu * \mathbb{1} = \varepsilon & \sigma_k = \mathbb{1} * P_k \\ \Lambda * \mathbb{1} = \log & \tau_k = \mathbb{1} * \tau_{k-1} \\ \varphi * \mathbb{1} = id & \sigma = \tau * \varphi \\ \mathbb{1} * \mathbb{1} = \tau & \ldots \end{array}}$$

Bsp.:
- $\varphi * \mathbb{1}(p^k) = \sum_{d \mid p^k} \varphi(d) = \varphi(1) + \varphi(p) + \varphi(p^2) + \ldots + \varphi(p^k)$
  $= 1 + (p-1) + (p^2 - p) + \ldots + (p^k - p^{k-1}) = p^k$.
- $\varphi * \mathbb{1}(1) = 1$ ✓

Häufig zeigen zth. Fktn. ein sehr sprunghaftes Verhalten, wie etwa τ_k bzw. $\tau = \tau_2$. Haben $\tau(p) = 2$ für jede PZ p, die Werte von τ sind andererseits unbeschränkt.

2.13. Kleine Werte von τ kommen ∞ oft vor, aber auch große Werte: Zu jedem $A > 0$ ex. ∞ viele n mit $\tau(n) > \log^A(n)$. ⌜Sei $r \in \mathbb{N}$ mit $r > A+1$, betr. p.w.v. $p_1, \ldots, p_r$ prim, $q := p_1 p_2 \cdots p_r$ und $n = q^v$ für $v \in \mathbb{N}$, dann ist $\frac{\tau(q^v)}{\log^A(q^v)} \geq \frac{(v+1)^r}{(\log q^v)^{r-1}} = \frac{(v+1)^r}{v^{r-1}} (\log q)^{1-r} > 1$ für $v \geq v_0$.⌟

Trotzdem zeigen zth. Funktionen oft im Mittelwert ein sehr regelmäßiges Verhalten, das sich normalerweise in Form einer asymptotischen Formel ausdrücken lässt.

Zeigen in AnZ 17:

2.14. • $\sum_{n \leq x} \tau(n) = x \log(x) + (2\gamma - 1)x + O(\sqrt{x})$, ⌜mit Dirichlet-Hyperbelmethode⌟

"O-Notation" s. AnZ 3

γ ist die Eulersche Konstante $\gamma = \lim_{x \to \infty} \left(\sum_{n \leq x} \frac{1}{n} - \log x \right) = 0.5772\ldots$

↳ "im Mittel" haben die nat. Zahlen $n \leq x$ etwa $\log(x)$ viele Teiler!

Denn $\frac{1}{\lfloor x \rfloor} \sum_{n \leq x} \tau(n)$ ist genau deren Mittelwert. Es lohnt sich nämlich oft, anstelle der eigentlichen zth. Fkt. deren Mittelwert zu studieren.