

## 2 Arithmetische Funktionen

### 2.1 Einführung

**Erklärung:** Eine zahlentheoretische Funktion ist eine Abbildung  $\alpha : \mathbb{N} \rightarrow \mathbb{C}$ , also nichts anderes als eine Folge  $\alpha_n = \alpha(n)$  komplexer Zahlen ( $n \in \mathbb{N}$ ).

#### Beispiel

$p_n: n \rightarrow p_n$  ( $n$ -te Primzahl) ist eine zahlentheoretische Funktion.

Kurzbezeichnung:  $\sum_{d|n} = \sum_{\{d \in \mathbb{N}_+ \mid d|n\}}$

Standardbezeichnungen (in vielen Büchern):

- $\varphi(n) = \#\{x \in \mathbb{N} \mid 1 \leq x \leq n \wedge \text{ggT}(x, n) = 1\}$  („Eulersche Funktion“)
- $\tau(n) = \sum_{d|n} 1 = \#\{x \in \mathbb{N}; x|n\}$
- $\sigma(n) = \sum_{d|n} d$  „Teilersumme“
- $\sigma_k(n) = \sum_{d|n} d^k$ ,  $k \in \mathbb{N}$ , also  $\sigma_0 = \tau$ ,  $\sigma_1 = \sigma$
- $\omega(n) = \#\{p \in \mathbb{P} \mid p|n\}$
- $\mu(n) = \begin{cases} 0 & \exists p \in \mathbb{P} : p^2|n \\ (-1)^{\omega(n)} & \text{sonst, d.h. „}n \text{ quadratfrei“} \end{cases}$  „Möbiusfunktion“

**Zeichen in dieser Vorlesung:**

- $c_a$ : Konstante Funktion, also  $\forall n \in \mathbb{N} : c_a(n) = a$
- $\delta: \delta(n) = \begin{cases} 1 & n = 1 \\ 0 & \text{sonst} \end{cases} = \delta_{1,n}$  „Kronecker-Delta“
- $\Pi_k(n) = n^k$  „Potenzfunktion“

Sprechweise für den Fall  $\text{ggT}(x, n) = 1 \iff x$  und  $n$  sind „relativ prim“.

#### Beispiel

(1)  $\varphi(12) = \#\{1, 5, 7, 11\} = 4$

(2)  $p \in \mathbb{P}$ ,  $n \in \mathbb{N}_+$ ,  $\varphi(p^n) = ?$

$$\begin{aligned} \text{ggT}(x, p^n) = 1 &\iff p \nmid x \\ \{x \in \mathbb{N}_+ \mid \text{ggT}(x, p^n) = 1, x \leq p^n\} &= \{x \in \mathbb{N}_+ \mid p \nmid x, x \leq p^n\} \\ &= \{1, \dots, p^n\} \setminus \{p, 2p, \dots, p^n\} = \{1, \dots, p^n\} \setminus p\{1, 2, \dots, p^{n-1}\} \\ \varphi(p^n) &= p^n - p^{n-1} = p^{n-1}(p - 1) = p^n(1 - \frac{1}{p}) \end{aligned}$$

## 2.2 Dirichlet-Reihen

Benannt nach Peter Gustav Lejeune Dirichlet, 1805-59.

### Definition

Sei  $\alpha$  eine zahlentheoretische Funktion. Ist  $s \in \mathbb{R}$  oder besser  $s \in \mathbb{C}$ , so definiert man:

$$L(s, \alpha) = \sum_{n \in \mathbb{N}_+} \frac{\alpha(n)}{n^s}$$

### Beispiel

$L(s, c_1) = \zeta(s)$  („Riemanns  $\zeta$ -Funktion“)

Wir rechnen nun formal.  $\alpha, \beta$  seien zahlentheoretische Funktionen:

$$\begin{aligned} L(s, \alpha) \cdot L(s, \beta) &= \sum_{n \in \mathbb{N}_+} \frac{\alpha(n)}{n^s} \cdot \sum_{n \in \mathbb{N}_+} \frac{\beta(n)}{n^s} \\ &= \sum_{n, u \in \mathbb{N}_+} \sum_{n, u; nu=m} \frac{\alpha(n) \cdot \beta(u)}{(nu)^s} \\ &= \sum_{m \in \mathbb{N}_+} \frac{(\alpha * \beta)(m)}{m^s} \end{aligned}$$

mit der *Dirichlet-Faltung*:

$$(\alpha * \beta)(n) = \sum_{u, v \in \mathbb{N}_+; uv=n} \alpha(u)\beta(v) = \sum_{d|n} \alpha(d)\beta\left(\frac{n}{d}\right)$$

Als Ergebnis erhalten wir jetzt (formal):

$$L(s, \alpha) \cdot L(s, \beta) = L(s, \alpha * \beta)$$

## 2.3 Arithmetische Funktionen allgemein

$R$  sei jetzt ein faktorieller Ring.

### Definition

$$R_{\text{nor}} = \{q_{\text{nor}} | q \neq 0\}$$

(z.B.:  $\mathbb{Z}_{\text{nor}} = \mathbb{N}_+$ )

**Bemerkung:**  $\{d|n | d \in R_{\text{nor}}\}$ , ( $n \neq 0$ ), ist endlich.

$n = e(n) \cdot \prod_{p \in \mathbb{P}} p^{v_p(n)}$  hat endlich viele  $v_p(n) \neq 0$ , etwa  $p = p_1, \dots, p_l$

$d|n, d = \prod_{p \in \mathbb{P}} p^{m_p}$  mit  $m_p \leq v_{p_1}(n), \dots, m_{p_l} \leq v_{p_l}(n)$ ,  $m_p = 0$  sonst.

**Definition**

(1) Jede Abbildung  $\alpha : R_{\text{nor}} \rightarrow K$  ( $K$  ein Körper) heißt in dieser Vorlesung ( $K$ -wertige) arithmetische Funktion (auf  $R$ ). Die Menge dieser Funktionen wird hier mit  $\text{Arfun} = \text{Arfun}_{R,K}$  bezeichnet.

(2) Für  $\alpha, \beta \in \text{Arfun}$  wird definiert:

- $\alpha + \beta$  durch  $(\alpha + \beta)(n) = \alpha(n) + \beta(n)$
- $c\alpha$ , ( $c \in K$ ), durch  $(c\alpha)(n) = c \cdot \alpha(n)$

(3) Dirichlet-Faltung  $\alpha * \beta$  durch

$$(\alpha * \beta)(n) = \sum_{d|n} \alpha(d) \cdot \beta\left(\frac{n}{d}\right)$$

(Das Inverse wird mit  $\alpha^{-1}$  bezeichnet, also  $\alpha * \alpha^{-1} = 1$ )

**Satz 2.1 (Arfun-Ring-Satz)**

- $(\text{Arfun}, +, *)$  ist *integrer* Ring und  $K$ -Vektorraum.
- $\alpha \in \text{Arfun}^\times \iff \alpha(1) \neq 0$ .

**Beweis**

Die Vektorraumeigenschaft wird wie in der Analysis gezeigt. Wir zeigen die Ringeigenschaft:

Einselement ist  $1_{\text{Arfun}} = \delta$ :

$$(\delta * \alpha)(n) = \sum_{d|n} \delta(d) \alpha\left(\frac{n}{d}\right) = \delta(1) \cdot \alpha\left(\frac{n}{1}\right) = \alpha(n)$$

Die Kommutativität von  $*$  ist offensichtlich. Die Distributivregel gilt auch:

$$\begin{aligned} \alpha * (\beta + \gamma)(n) &= \sum_{d|n} \alpha(d) \cdot (\beta + \gamma)\left(\frac{n}{d}\right) \\ &= \sum_{d|n} \alpha(d) \cdot \left(\beta\left(\frac{n}{d}\right) + \gamma\left(\frac{n}{d}\right)\right) \quad (\cdot \text{ ist distributiv in } \mathbb{C}) \\ &= \sum_{d|n} \left(\alpha(d) \cdot \beta\left(\frac{n}{d}\right) + \alpha(d) \cdot \gamma\left(\frac{n}{d}\right)\right) \\ &= \sum_{d|n} \alpha(d) \cdot \beta\left(\frac{n}{d}\right) + \sum_{d|n} \alpha(d) \cdot \gamma\left(\frac{n}{d}\right) \\ &= (\alpha * \beta)(n) + (\alpha * \gamma)(n) \\ &= ((\alpha * \beta) + (\alpha * \gamma))(n) \end{aligned}$$

Bemerkung:

$$(\alpha * \beta)(n) = \sum_{u,v \in R_{\text{nor}}; u \cdot v = n} \alpha(u) \beta(v)$$

Nun zeigen wir noch die Assoziativregel:

$$\begin{aligned}
 ((\alpha * \beta) * \gamma)(n) &= \sum_{u,v; uv=n} (\alpha * \beta)(u) \gamma(v) \\
 &= \sum_{uv=n; xy=u} (\alpha(x) \beta(y)) \gamma(v) \\
 &= \sum_{xyv=n} \alpha(x) \beta(y) \gamma(v) \\
 &= \sum_{xu=n; yv=u} \alpha(x) (\beta(y) \gamma(v)) \\
 &= \sum_{xu=n} \alpha(x) ((\beta * \gamma)(u)) \\
 &= (\alpha * (\beta * \gamma))(u)
 \end{aligned}$$

Den Beweis, dass Arfun ein integrierter Ring ist, führen wir nur für  $R = \mathbb{Z}$ , lässt sich aber mit etwas Scharfsinn auf beliebige  $R$  übertragen.

$$\alpha \neq 0, \beta \neq 0 \implies \exists u = \min\{x \in \mathbb{N}_+ | \alpha(x) \neq 0\}, v = \min\{y \in \mathbb{N}_+ | \beta(y) \neq 0\}. n := uv.$$

$$(\alpha * \beta)(n) = \sum_{xy=n} \alpha(x) \beta(y). x < u \implies \alpha(x) = 0, x > u \implies y = \frac{n}{x} < \frac{n}{u} = v \implies \beta(y) = 0.$$

$$\text{Also: } (\alpha * \beta)(n) = \alpha(u) \beta(\frac{n}{u}) = \alpha(u) \beta(v) \neq 0, \text{ da } K \text{ integer} \implies \alpha * \beta \neq 0$$

$$\text{Die Existenz von Inversen: } \alpha \in \text{Arfun}^\times \iff \exists \beta \in \text{Arfun} : \beta * \alpha = \delta (= 1_{\text{Arfun}})$$

$$\beta \text{ existiere} \implies 1 = \delta(1) = (\beta * \alpha)(1) = \sum_{d|1} \beta(d) \alpha(\frac{1}{d}) = \beta(1) \alpha(1) \implies \alpha(1) \neq 0$$

Sei  $\alpha(1) \neq 0$ . Setze  $\beta(1) = \frac{1}{\alpha(1)}$  (geht, da  $K$  ein Körper ist und  $\alpha(1) \neq 0$ ).  $\beta$  ist so zu definieren, dass für  $n \in R_{\text{nor}}, n \neq 1$ , gilt:

$$(*) \quad 0 = \delta(n) = (\beta * \alpha)(n) = \sum_{d|n} \beta(d) \alpha(\frac{n}{d}) \quad (2.1) \quad \blacksquare$$

Induktion nach  $\text{len}(n) = \sum_{p \in \mathbb{P}} v_p(n)$ ,  $\text{len}(n) = 0$ , dann  $n = 1$ , also OK.

Bemerkung:  $d|n, d \neq n (d = d_{\text{nor}}) \implies \text{len}(d) < \text{len}(n)$

Induktiv darf man  $\beta(d)$  schon als definiert annehmen.

$$(2.1) \iff \beta(n) = -\frac{1}{\alpha(1)} \sum_{d|n, d \neq n} \beta(d) \alpha(\frac{n}{d}).$$

Die rechte Seite ist schon erklärt, die linke Seite dadurch gewonnen.  $\beta$  also rekursiv, also definiert, so dass  $\beta * \alpha = \delta$ . Im Prinzip wird  $\beta$  als „Programm“ realisiert.

## 2.4 Multiplikative arithmetische Funktionen

### Definition

$\alpha \in \text{Arfun}_{R,K}, (\alpha \neq 0)$ , heie *multiplikativ*  $\iff$

$$\forall m, n \in R_{\text{nor}} \text{ mit } \text{ggT}(m, n) = 1 : \quad \alpha(mn) = \alpha(m) \alpha(n)$$

$$\alpha \text{ multiplikativ} \implies \alpha\left(\prod_{p \in \mathbb{P}} p^{v_p(n)}\right) = \prod_{p \in \mathbb{P}} \alpha(p^{v_p(n)})$$

Ein Beispiel für eine Anwendung folgt aus der Multiplikativität der Eulerfunktion  $\varphi$ , welche wir später zeigen werden:

$$\varphi(p^{v_p(n)}) = p^{v_p(n)} \left(1 - \frac{1}{p}\right) \text{ für } p \in \mathbb{P} \implies \varphi(n) = n \cdot \prod_{p \in \mathbb{P}, p|n} \left(1 - \frac{1}{p}\right) \quad \text{„Eulers Formel“}$$

### Beispiel

$\Pi_k$  ist multiplikativ. ( $\Pi_k(n) = n^k$ )

### Satz 2.2 (Multiplikativitätssatz für Arfun)

- (1) Ist  $\alpha \in \text{Arfun}$  multiplikativ, so ist  $\alpha(1) = 1$
- (2) Die multiplikativen Funktionen bilden eine Untergruppe von  $(\text{Arfun}^\times, *)$ , also  $\alpha, \beta$  multiplikativ, so auch  $\alpha * \beta$  und  $\alpha^{-1}$ .

### Beweis

- (1)  $\alpha$  ist multiplikativ  $\implies \alpha(1) = \alpha(1 \cdot 1) \stackrel{\text{ggT}(1,1)=1}{=} \alpha(1) \cdot \alpha(1) \stackrel{\text{Körper!}}{\implies} \alpha(1) = 1 \text{ oder } \alpha(1) = 0$ .  
Falls  $\alpha(1) = 0$ , so  $\forall n \in R_{\text{nor}} \alpha(n) = \alpha(n \cdot 1) \stackrel{\text{ggT}(n,1)=1}{=} \alpha(n) \cdot \underbrace{\alpha(1)}_{=0} = 0 \implies \alpha \equiv 0$  und das ist nach Definition *nicht* multiplikativ, also gilt  $\alpha(1) = 1$ .
- (2) Zu zeigen:  $\alpha, \beta$  multiplikativ  $\implies \alpha * \beta$  multiplikativ und  $\alpha^{-1}$  ist ebenfalls multiplikativ.

$$(\alpha * \beta)(n_1 n_2) = (\alpha * \beta)(n_1) \cdot (\alpha * \beta)(n_2), \quad (2.2)$$

falls  $\text{ggT}(n_1, n_2) = 1$ .  $(\alpha * \beta)(1) = \sum_{d|1} \alpha(d) \beta(\frac{1}{d}) = \alpha(1) \beta(1) \stackrel{\alpha, \beta \text{ mult.}}{=} 1 \cdot 1 \implies (2.2)$  ist ok, wenn  $n_1 = 1$  oder  $n_2 = 1$ . Sei nun  $n_1 \neq 1, n_2 \neq 1$ .

**Behauptung:**  $n = n_1 n_2$ : Jeder Teiler  $d|n$  ist eindeutig in der Form  $d = d_1, d_2$  mit  $d_1|n_1$  und  $d_2|n_2$  darstellbar.

Folgende Funktion  $f$  ist bijektiv:

$$f : \begin{cases} \{(d_1, d_2) | d_1|n_1, d_2|n_2\} & \rightarrow \{d|n\} \\ (d_1, d_2) & \mapsto d_1 d_2 \end{cases}$$

Die Behauptung ist klar, wenn man die Primzahlzerlegung anschaut ( $n_1, n_2 \neq 1$ ):

$n_1 = \prod_{i=1}^t p_i^{v_i}, n_2 = \prod_{i=1}^l q_i^{w_i}$ , die  $p_i$  sowie die  $q_i$  sind jeweils paarweise verschiedene Primzahlen.  $\text{ggT}(n_1, n_2) = 1 \iff \{p_1, p_2, \dots, p_t\} \cap \{q_1, q_2, \dots, q_l\} = \emptyset$ .

$$d|n, d = \underbrace{\prod_{i=1}^t p_i^{u_i}}_{=d_1} \cdot \underbrace{\prod_{i=1}^l q_i^{y_i}}_{=d_2} \text{ mit } u_j \leq v_j, y_k \leq w_k.$$

Es gilt weiterhin  $\text{ggT}(d_1, d_2) = 1 = \text{ggT}\left(\frac{n_1}{d_1}, \frac{n_2}{d_2}\right)$ .

$$\begin{aligned}
 (\alpha * \beta)\left(\underbrace{n}_{=n_1 n_2}\right) &= \sum_{d|n} \alpha(d) \beta\left(\frac{n}{d}\right) \\
 &= \sum_{d_1|n_1, d_2|n_2} \alpha(d_1 d_2) \beta\left(\frac{n_1}{d_1} \frac{n_2}{d_2}\right) \\
 &\stackrel{\alpha, \beta \text{ mult.}}{=} \sum_{d_1|n_1, d_2|n_2} \alpha(d_1) \alpha(d_2) \beta\left(\frac{n_1}{d_1}\right) \beta\left(\frac{n_2}{d_2}\right) \\
 &= \sum_{d_1|n_1, d_2|n_2} \left(\alpha(d_1) \beta\left(\frac{n_1}{d_1}\right)\right) \cdot \left(\alpha(d_2) \beta\left(\frac{n_2}{d_2}\right)\right) \\
 &\stackrel{\text{distributiv}}{=} \sum_{d_1|n_1} \alpha(d_1) \beta\left(\frac{n_1}{d_1}\right) \cdot \sum_{d_2|n_2} \alpha(d_2) \beta\left(\frac{n_2}{d_2}\right) \\
 &= (\alpha * \beta)(n_1) \cdot (\alpha * \beta)(n_2).
 \end{aligned}$$

Zeige nun noch:  $\alpha$  multiplikativ  $\implies \beta = \alpha^{-1}$  ist multiplikativ. In der Vorlesung wird nur die Idee gezeigt, der Rest bleibt als Übung. Sei also  $\gamma$  die multiplikative Funktion mit  $\gamma(1) = 1$  und  $\gamma(p^k) = \beta(p^k)$ , ( $p \in P, k \in \mathbb{N}_+$  (nach (3))) Mit Hilfe der Multiplikativität von  $\gamma$  leicht nachzuweisen:  $\alpha * \gamma = \delta \implies \gamma = \alpha^{-1} = \beta \implies \beta$  ist multiplikativ. ■

### Beispiel

Anwendungsbeispiele für diesen Satz:  $\Pi_k$  ist multiplikativ,  $c_1 = \Pi_0$  auch. Daraus folgt, dass  $\Pi_k * c_1$  auch multiplikativ ist. Wegen  $(\Pi_k * c_1)(n) = \sum_{d|n} \Pi_k(d) c_1\left(\frac{n}{d}\right) = \sum_{d|n} d^k = \sigma_k(n)$  ist also auch  $\sigma_k$ , insbesondere  $\sigma$  und  $\tau$ , multiplikativ.

Zum Beispiel:  $\sigma_k(p^t) = \sum_{d|p^t} d^k = \sum_{j=0}^t (p^j)^k = \frac{p^{k(t+1)} - 1}{p^k - 1}$ .

Das liefert die Formel  $\sigma_k(n) = \prod_{p \in \mathbb{P}, p|n} \frac{p^{k(v_p(n)+1)} - 1}{p^k - 1}$  sowie  $\tau(p^t) = t + 1 \implies \tau(n) = \prod_{p|n} (v_p(n) + 1)$  und

$$\sigma(n) = \prod_{p|n} \frac{p^{v_p(n)+1} - 1}{p - 1}. \quad (2.3)$$

Eine konkrete Berechnung ist  $\sigma(100) = \frac{2^3-1}{2-1} \cdot \frac{5^3-1}{5-1} = 7 \cdot 31$ .

### Historischer Exkurs

$\sigma(n) = \sum_{d|n} d$  (Teilersumme),  $\sigma^*(n) = \sum_{d|n, d \neq n} d = \sigma(n) - n$ .

**Benennung (Griechen):**  $n \in \mathbb{N}_+$  heißt  $\left\{ \begin{array}{l} \text{defizient} \\ \text{abundant} \\ \text{vollkommen} \end{array} \right\} \iff \sigma^*(n) \left\{ \begin{array}{l} < \\ > \\ = \end{array} \right\} n$ .

Beispielsweise ist jede Primzahl defizient, 12 abundant und 6 ist die kleinste vollkommene Zahl.

**Satz 2.3 (Euklid, Euler)**

Die geraden vollkommenen Zahlen sind genau die der Form

$$n = 2^{p-1} M_p \quad p \in \mathbb{P}, \quad M_p = 2^p - 1 \in \mathbb{P} \text{ Mersenne-Primzahl.}$$

Unbekannt: Gibt es unendlich viele Mersenne-Primzahlen? Gibt es unendlich viele vollkommene Zahlen? Gibt es wenigstens *eine* ungerade vollkommene Zahl (Es gibt mindestens 100 Arbeiten zu den Eigenschaften der ungeraden vollkommenen Zahlen, aber leider hat noch niemand eine gefunden)?

**Beweis**

„ $\Leftarrow$ “ Sei  $n = 2^{p-1} M_p$  wie oben.

$$\begin{aligned} \sigma(n) &= \sigma(2^{p-1}) \cdot \sigma(M_p) = \left( \underbrace{\frac{2^{p-1+1} - 1}{2 - 1}}_{\text{vgl. (2.3)}} \right) \cdot \underbrace{(1 + M_p)}_{M_p \text{ ist prim}} \\ &= (2^p - 1) 2^p = 2 \cdot 2^{p-1} \cdot M_p = 2n \implies \sigma^*(n) = n \implies n \text{ vollkommen.} \end{aligned}$$

„ $\Rightarrow$ “  $n$  sei vollkommen und  $2|n$ , also  $\sigma(n) = 2n$ .  $n = 2^r \cdot x$ ,  $x \in \mathbb{N}_+$ ,  $2 \nmid x \implies \text{ggT}(2^r, x) = 1$ .

$$\sigma(n) \stackrel{\text{mult.}}{=} \sigma(2^r) \sigma(x) = \frac{2^{r+1} - 1}{2 - 1} \sigma(x) \stackrel{n \text{ vollkommen}}{=} 2n = 2^{r+1} x \quad (2.4)$$

$\text{ggT}(2^{r+1}, 2^{r+1} - 1) = 1 \implies 2^{r+1} | \sigma(x)$ , also  $\sigma(x) = 2^{r+1} y$  mit  $y \in \mathbb{N}_+$

$\stackrel{(2.4)}{\implies} x = \underbrace{(2^{r+1} - 1)}_{=:b} y = by$ .  $T(x) \subseteq \{1, y, b, by\}$  mit  $b > 1$  wegen  $r > 0$ .  $\sigma(x) = (b+1)y = y + by$ ,  $y < by$  wegen  $b > 1$ .

$\implies T(x) = \{y, by\} \implies y = 1$ ,  $x = b$ ,  $T(x) = \{1, b\} = \{1, x\} \implies x = 2^{r+1} - 1$  ist prim.

Mit Aufgabe 3a, Übungsblatt 1  $\implies r+1 = p \in \mathbb{P}$ ,  $x = M_p \implies$  Behauptung. ■

**Satz 2.4 (ohne Beweis, nach Abdul Hassan Thâ bit Ibn Kurah, ca. 900)**

Sind  $u = 3 \cdot 2^{n-1} - 1$ ,  $v = 3 \cdot 2^n - 1$ ,  $w = 9 \cdot 2^{n-1}$  alle prim, so sind  $2^u u v$  und  $2^n w$  befreundet. Zwei Zahlen  $n, m$  aus  $\mathbb{N}_+$  heißen befreundet, genau wenn  $\sigma(n) = \sigma(m)$  gilt (zum Beispiel 220 und 284).

Zur Eulerschen Funktion  $\varphi$ :  $\text{Relp}(n, d) := \{x \in \mathbb{N}_+ | x \leq n, \text{ggT}(n, x) = d\}$ .

$\varphi(n) = \# \text{Relp}(n, 1)$ .

**Lemma 2.5 (Gauß)**

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

**Beweis**

Die Abbildung  $f : \begin{cases} \text{Relp}(\frac{n}{d}, 1) & \rightarrow & \text{Relp}(n, d) \\ x & \mapsto & dx \end{cases}$  ist bijektiv.

$\text{ggT}(\frac{n}{d}, x) = 1, d = d \cdot 1 = \text{ggT}(d \frac{n}{d}, d \cdot 1) = \text{ggT}(n, d), x \leq \frac{n}{d} \iff dx \leq n. \bigcup_{d|n} \text{Relp}(n, d) = \{1, 2, \dots, n\}$  (wenn  $\text{ggT}(y, n) = d$ , so  $y \in \text{Relp}(n, d), y \leq n$ ).

$n = \#\{1, 2, \dots, n\} = \sum_{d|n} \# \text{Relp}(n, d) \stackrel{\text{wg. obiger Bijektion}}{=} \sum_{d|n} \# \text{Relp}(\frac{n}{d}, 1) = \sum_{d|n} \varphi\left(\frac{n}{d}\right) = \sum_{d'|n} \varphi(d'), \quad (d' = \frac{n}{d}).$  ■

Lemma von Gauß sagt:  $\Pi_1 = \varphi * c_1, \Pi_1(n) = n^1 = n$ . Da  $\Pi_1$  und  $c_1$  multiplikativ sind  $\implies \varphi = \Pi_1 * c_1^{-1}$  ebenfalls multiplikativ (aus Multiplikativitätssatz)  $\implies \varphi(n) = n \Pi_{p_n}(1 - \frac{1}{p})$  (früher).

**Definition**

Ist  $\alpha \in \text{Arfun}$ , dann heißt  $\hat{\alpha}$  Möbiustransformierte von (oder Summatorische Funktion zu)  $\alpha$ , wenn:

$$\hat{\alpha}(n) := \sum_{d|n} \alpha(d)$$

(Das heißt:  $\hat{\alpha} = \alpha * c_1$ .)

Problem: Wie kann man  $\alpha$  aus  $\hat{\alpha}$  gewinnen (bzw. berechnen)?

Lösung:  $\hat{\alpha} = \alpha * c_1 \implies \alpha = \hat{\alpha} * \mu$ , mit  $\mu = c_1^{-1}$ .

$\mu = c_1^{-1}$  heißt Möbiusfunktion.

Rest: Bestimmung von  $\mu$ , da  $\mu$  multiplikativ ist, reicht es aus,

$\mu(p^l) = c_p, p \in P, l \in \mathbb{N}_+$  zu ermitteln.

$\mu(1) = 1$

$0 = \delta(p^l) = \mu * c_1(p^l) = \sum_{d|p^l} \mu(d) = \sum_{j=0}^l \mu(p^j)$

$l = 1 : 0 = \mu(1) + \mu(p) \implies \mu(p) = -1$

$l = 2 : 0 = \mu(1) + \mu(p) + \mu(p^2) \implies \mu(p^2) = 0$

...

$\mu(p^i) = 0$  für  $j \geq 2$ . Also folgt, weil  $\mu$  multiplikativ ist:

$$\mu(n) = \begin{cases} 0 & \exists p \in \mathbb{P} : p^2 | n, \text{ d.h. } n \text{ ist nicht quadratfrei} \\ (-1)^t & \text{falls } n = p_1 \cdot p_2 \cdot \dots \cdot p_t \text{ mit } t \text{ verschiedenen Primzahlen} \end{cases}$$

Ergebnis:

**Satz 2.6 (Umkehrrsatz von Möbius)**

Sei  $\alpha$  arithmetische Funktion,  $\hat{\alpha}$  die Möbiustransformierte von  $\alpha$ , dann gilt  $\alpha = \hat{\alpha} * \mu$  mit der Möbiusfunktion  $\mu$ , das heißt:

$$\alpha(n) = \sum_{d|n} \hat{\alpha}(d) \mu\left(\frac{n}{d}\right) \quad \text{Möbiussche Umkehrformel}$$

und  $\mu$  wie oben.

Lineraturhinweise zu den Arithmetischen Funktionen:



- (1) Für Algebra-Freunde: „Der Ring Arfun ist selbst faktoriell“, siehe Cashwell, Everett: The Ring of Numbertheoretic Functions, Pacific Math.J., 1955, S. 975ff.
- (2) Umkehrformeln gibt es für allgemeinere geordnete Mengen als  $(R_{\text{nor}}, |)$ , siehe Johnson, Algebra I.
- (3) Für Analysis-Freunde: Viel Analysis über zahlentheoretische Funktionen. Viele Sätze über asymptotisches Verhalten (ähnlich  $p_n \sim n \cdot \log n$ ), siehe Schwarz, Spieker, „Arithmetical functions“, Cambridge University Press, 1994.

