2. Zahlentheoretische Funktionen.

Sei Φ die Menge der Abbildungen $\mathbb{N} \to \mathbb{R}$, derartige Abbildungen nennt man *zahlentheoretische Funktionen* (oft betrachtet man allgemeiner Abbildungen mit Werten in $\mathbb{C}$).

Zahlentheoretische Funktionen, an denen wir interessiert sind:

$$\begin{array}{lllll} I(n) = 0 & \text{für} & n > 1 & \text{und} & I(1) = 1 \\ U(n) = 1 & \text{für} & n \geq 1 & & \\ E(n) = n & \text{für} & n \geq 1 & & \end{array}$$

$$\begin{aligned} \tau(n) &= (\text{Anzahl der Teiler von } n) \\ \sigma(n) &= (\text{Summe der Teiler von } n) \end{aligned}$$

Ganz wichtig ist die Eulersche ϕ-Funktion, die in 2.6 eingeführt wird, aber auch die Möbius-Funktion μ, siehe 2.5.

2.1. Die Faltung.

Wir definieren auf Φ ein Produkt $*$ (*Dirichlet-Produkt, Faltung*) auf folgende Weise: Seien $f, g \in \Phi$. Setze

$$(f * g)(n) = \sum_{d|n} f(d) g(\frac{n}{d}) = \sum_{d_1 d_2 = n} f(d_1) g(d_2)$$

(dabei bedeutet die letzte Summenbildung, dass über alle Paare $(d_1, d_2) \in \mathbb{N}^2$ summiert werden soll, für die $d_1 d_2 = n$ gilt). Beispielsweise gilt:

$$\boxed{\tau = U * U, \quad \sigma = E * U.}$$

Ist f eine beliebige zahlentheoretische Funktion, so betrachtet man oft $f * U$ und nennt dies die zugehörige *summatorische* Funktion: beachte, dass $(f * U)(n) = \sum_{d|n} f(d)$, es wird hier also die Summe der Werte $f(d)$ für alle Teiler d von n gebildet.

2.1.1. *Die Menge Φ ist bezüglich $*$ eine kommutative Halbgruppe mit neutralem Element I.*

Beweis: Übungsaufgabe! Zum Assoziativgesetz sollte man anmerken: Seien f, g, h zahlentheoretische Funktionen. Dann ist $(f * g * h)(n) = \sum_{d_1, d_2, d_3} f(d_1) g(d_2) h(d_3)$, wobei man über alle Tripel (d_1, d_2, d_3) mit $d_1 d_2 d_3 = n$ summiert.

Zusatz (Übungsaufgabe 4.1): Nehmen wir zusätzlich noch auf Φ die punktweise Addition als Addition, so erhalten wir einen kommutativen Ring.

2.1.2. *Eine Funktion $f \in \Phi$ ist genau dann bezüglich $*$ invertierbar, wenn $f(1) \neq 0$ gilt.*

Beweis: Sei $f * g = I$. Dann ist $1 = I(1) = f(1)g(1)$, da $n = 1$ nur den einzigen Teiler $d = 1$ hat. Aus $f(1)g(1) = 1$ folgt, dass $f(1)$ nicht Null sein kann. Umgekehrt sei nun f eine zahlentheoretische Funktion mit $f(1) \neq 0$. Wir definieren eine zahlentheoretische Funktion g induktiv wie folgt: sei $g(1) = f(1)^{-1}$. Sei nun $n \geq 2$ und seien schon die Werte $g(1), \ldots, g(n-1)$ definiert. Wir setzen

$$g(n) = -f(1)^{-1} \sum\nolimits_{d|n, d<n} g(d) f(\tfrac{n}{d})$$

(die Summierung erfolgt also über alle Teiler d von n mit $d < n$; für derartige Zahlen d ist ja $g(d)$ schon definiert). Auf diese Weise erhalten wir eine Funktion g mit $g(1)f(1) = 1 = I(1)$ und

$$I(n) = 0 = g(n)f(1) + \sum\nolimits_{d|n, d<n} g(d) f(\tfrac{n}{d}) = (g * f)(n)$$

für $n \geq 2$. Es ist also $g = f^{-1}$.

2.2. Multiplikative Funktionen. Wir interessieren uns vor allem für "multiplikative" Funktionen: Eine Funktion $f \in \Phi$ heißt *multiplikativ*, falls f nicht die Nullfunktion ist und falls gilt: Sind n, n' teilerfremd, so ist $f(nn') = f(n)f(n')$. (Insbesondere gilt dann $f(1) = 1$; denn wäre $f(1) = 0$, so wäre f wegen $f(1 \cdot n) = f(1)f(n)$ die Nullfunktion, dies ist ausgeschlossen; aus $f(1) = f(1 \cdot 1) = f(1)f(1)$ und $f(1) \neq 0$ folgt aber $f(1) = 1$.)

Warnung: In der Algebra würde man eine Funktion nur dann "multiplikativ" nennen, wenn die Regel $f(nn') = f(n)f(n')$ für **alle** n, n' gilt, nicht nur für teilerfremde Paare. In der Zahlentheorie heißen derartige Funktionen "vollständig multiplikativ", diese Klasse von Funktionen spielt aber keine große Rolle! Beachte: Sind die Funktionen f, g vollständig multiplikativ, so ist $f * g$ multiplikativ, meist aber **nicht** vollständig multiplikativ. Beispiel: die Funktion U ist vollständig multiplikativ. Aber $\tau := U * U$ ist nicht vollständig multiplikativ ($\tau(n)$ ist die Anzahl der Teiler von n, und es ist $\tau(2) = 2$, und $\tau(4) = 3 \neq 2^2 = \tau(2)^2$).

Offensichtlich gilt für f multiplikativ: Kennt man die Werte $f(p^e)$, für alle Primzahlen p und alle natürlichen Zahlen e, so kennt man f, denn für $n = p_1^{e_1} \cdots p_t^{e_t}$ mit paarweise verschiedenen Primzahlen $p_1, \ldots, p_t$ gilt

$$f(p_1^{e_1} \cdots p_t^{e_t}) = f(p_1^{e_1}) \cdots f(p_t^{e_t}).$$

Umgekehrt kann man eine multiplikative Funktion g dadurch definieren, dass man beliebige Werte $g(p^e)$ (für p Primzahl, $e \in \mathbb{N}$) wählt, und diese Abbildung "multiplikativ fortsetzt":

$$g(p_1^{e_1} \cdots p_t^{e_t}) = g(p_1^{e_1}) \cdots g(p_t^{e_t})$$

(für paarweise verschiedene Primzahlen $p_1, \ldots, p_t$ und alle $e_i \in \mathbb{N}$).

2.2.1. *Sind f, g muliplikativ, ist ist auch $f * g$ multiplikativ.*

Beweis: Seien n_1, n_2 teilerfremde natürliche Zahlen. Ist d ein Teiler von $n_1 n_2$, so lässt sich d eindeutig in der Form $d = d_1 d_2$ mit $d_1 | n_1$ und $d_2 | n_2$ schreiben (es ist $d_1 = (d, n_1)$ und $d_2 = (d, n_2)$). Da n_1, n_2 teilerfremde Zahlen sind, sind auch die Zahlen d_1, d_2 teilerfremd. Entsprechend sind auch die Zahlen n_1/d_1 und n_2/d_2 teilerfremd.

$$\begin{aligned}(f*g)(n_1n_2) &= \sum_{d|n_1n_2} f(d)g\big(\frac{n_1n_2}{d}\big)\\ &= \sum_{d_1,d_2} f(d_1d_2)g\big(\frac{n_1}{d_1}\frac{n_2}{d_2}\big)\\ &\underset{(*)}{=} \sum_{d_1,d_2} f(d_1)f(d_2)g\big(\frac{n_1}{d_1}\big)g\big(\frac{n_2}{d_2}\big)\\ &= \Big(\sum_{d_1} f(d_1)g\big(\frac{n_1}{d_1}\big)\Big)\Big(\sum_{d_2} f(d_2)g\big(\frac{n_2}{d_2}\big)\Big)\\ &= (f*g)(n_1)\cdot(f*g)(n_2),\end{aligned}$$

dabei gilt das Gleichheitszeichen mit $(*)$, weil f und g multiplikativ sind.

2.2.2. *Ist f multiplikativ und $f(1) \neq 0$, so ist auch f^{-1} multiplikativ.*

Beweis. Definiere g wie folgt: Es sei $g(p^j) = f^{-1}(p^j)$ für jede Primzahl p und $j \in \mathbb{N}$ (nach Voraussetzung ist f invertierbar), und wir setzen diese Abbildung multiplikativ fort. Auf diese Weise erhalten wir eine multiplikative Funktion g. Da f, g multiplikativ sind, ist nach 2.2.1 auch $f * g$ multiplikativ. Wir zeigen: $f * g = I$. Da die beiden Funktionen $f * g$ und I multiplikativ sind, brauchen wir nur $(f * g)(p^e) = I(p^e)$ für Primzahlpotenzen p^e zu zeigen. Es ist

$$\begin{aligned}(f*g)(p^e) &= \sum\nolimits_{0\le e'\le e} f(p^{e'})g(p^{e-e'})\\ &\underset{(*)}{=} \sum\nolimits_{0\le e'\le e} f(p^{e'})f^{-1}(p^{e-e'})\\ &= (f*f^{-1})(p^e) = I(p^e),\end{aligned}$$

dabei gilt $(*)$, da $p^{e-e'}$ eine p-Potenz ist, und die Abbildungen g und f^{-1} nach der Definition von g auf p-Potenzen übereinstimmen.

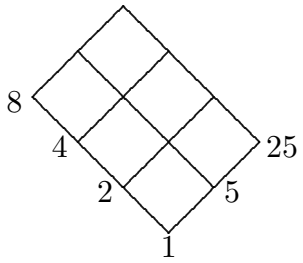
Die Funktionen I, U, E sind offensichtlich multiplikativ, also sind auch τ und σ multiplikativ.

2.3. Die Funktion τ. Es ist $\tau(p^e) = e + 1$, also gilt

$$\boxed{\tau(p_1^{e_1} \cdots p_t^{e_t}) = \prod_{i=1}^{t}(e_i + 1)}$$

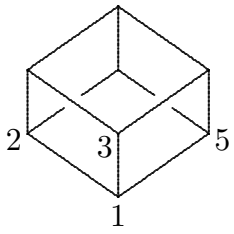
(falls $p_1, \ldots, p_t$ paarweise verschiedene Primzahlen sind).

Beispiel 1. $\tau(200) = \tau(2^3 5^2) = 4 \cdot 3 = 12$. Zugehöriges Schokoladen-Bild:



Die Teiler bilden ein Rechtecksraster, beschriftet wurden nur die beiden unteren Kanten (hier findet man alle Primpotenzteiler) — die weitere Beschriftung erhält man durch die jeweiligen Produkt-Bildungen. Ganz allgemein gilt: Ist $n = p_1^{e_1} p_2^{e_2}$ mit Primzahlen $p_1 \neq p_2$, so bilden die Teiler ein derartiges Rechteck.

Beispiel 2. $\tau(2 \cdot 3 \cdot 5) = 2 \cdot 2 \cdot 2 = 8$. Zugehöriges Würfelbild:



2.4. Die Funktion σ. Es ist

$$\boxed{\sigma(p^e) = \frac{p^{e+1} - 1}{p - 1}}$$

,

Beweis: Die Zahl p^e hat die Teiler $p^{e'}$ mit $0 \leq e' \leq e$ und deren Summe ist

$$\sum\nolimits_{0 \leq e' \leq e} p^{e'} = 1 + p + \cdots + p^e = \frac{p^{e+1} - 1}{p - 1}.$$

2.5. Die Möbius-Funktion μ. Die Funktion U ist nach 2.1.2 invertierbar. Setze $\mu = U^{-1}$, man nennt dies die *Möbius'sche Umkehrfunktion.* Die Funktion μ wird vor allem wegen der trivialerweise geltenden Formel

$$\boxed{f = (f * U) * \mu}$$

gebraucht — diese Formel besagt: *Kennt man die summatorische Funktion $f * U$, so kann man durch Faltung mit μ die Funktion f zurück gewinnen.*

Andere Formulierung:

$$\boxed{\text{Ist} \quad F(n) = \sum\nolimits_{d|n} f(d), \quad \text{so ist} \quad f(n) = \sum\nolimits_{d|n} F(d)\mu(\frac{n}{d}).}$$

2.5.1. *Die Funktion $\mu = U^{-1}$ ist multiplikativ* (wegen 2.2.2).

2.5.2. Wir berechnen die Werte $\mu(p^e)$. Es ist $\mu(p) = -1$ und $\mu(p^e) = 0$ für $e > 1$.

Beweis: Es ist $\mu(1) = 1$. Für $e \geq 1$ gilt

$$0 = I(p^e) = (U * \mu)(p^e) = \sum\nolimits_{0 \leq i \leq e} \mu(p^i).$$

Für $e = 1$ liefert dies $0 = \mu(1) + \mu(p) = 1 + \mu(p)$, also $\mu(p) = -1$. Für $e \geq 2$ sehen wir:

$$0 = \sum\nolimits_{0 \leq i \leq e} \mu(p^i) \qquad \text{und auch} \qquad 0 = \sum\nolimits_{0 \leq i < e} \mu(p^i),$$

also ist $\mu(p^e) = 0$.

Also erhalten wir die Formel:

$$\boxed{\mu(n) = \begin{cases} 0 & \text{falls } n \text{ nicht quadratfrei,} \\ (-1)^t & \text{falls } n = p_1 \cdots p_t \text{ mit paarweise verschiedenen Primzahlen } p_i. \end{cases}}$$

dabei schließt die zweite Zeile auch den Fall $n = 1$, also $t = 0$ ein: Es ist $\mu(1) = 1$.

2.5.3. Die Mertens'sche "Vermutung".

Betrachtet wird die Funktion $\sum_{n \leq x} \mu(n)$. Offensichtlich ist $|\sum_{n \leq x} \mu(n)| \leq x$ und Mertens vermutete 1897, dass sogar gelten sollte:

$$|\sum\nolimits_{n \leq x} \mu(n)| \leq \sqrt{x}$$

(er bestätigte dies für $x \leq 10\,000$). Odlyzko und te Riele zeigten 1983, dass die Behauptung falsch ist: sie zeigten, dass es Gegenbeispiele geben muss. Pintz zeigte 1987, dass es ein Gegenbeispiel $x \leq \exp(3,21 \cdot 10^{64})$ geben muss. Genaueres weiß man aber nicht!

2.6. Die Eulersche ϕ-Funktion. Definition:

$$\phi(n) = (\text{Anzahl der Zahlen } 1 \leq m \leq n \text{ mit } (m,n) = 1)$$

2.6.1. *Es ist*

$$\boxed{\phi * U = E.}$$

Beweis: Sei $F(d)$ die Menge der natürlichen Zahlen $a \leq d$ mit $(a,d) = 1$. Es ist also $\phi(d) = |F(d)|$. Ist m eine natürliche Zahl, so liefert die Multiplikation mit m eine injektive Abbildung $F(d) \to \{1, 2, \ldots, md\}$ und zwar erhält man genau die Zahlen b mit $1 \leq b \leq md$ und $(b, md) = m$.

Fangen wir umgekehrt mit $[1,n] = \{1, 2, \ldots, n\}$ an, und bezeichnen wir mit $T(n)$ die Menge der Teiler von n, so können wir die Abbildung $f = (-,n)\colon [1,d] \to T(n)$ betrachten — sie ordnet jedem b mit $1 \leq b \leq n$ den größten gemeinsamen Teiler (b,n) zu. Für $n = d_1 d_2$ ist $f^{-1}(d_1) = d_1 F(d_2)$ (dies ist die Menge der Zahlen $1 \leq b \leq n$ mit größtem gemeinsamen Teiler $(b,n) = d_1$.

2.6.2. Folgerung: *ϕ ist multiplikativ.* Denn $\phi = E * \mu$, und E und μ sind multiplikativ.

2.6.3. *Es ist $\phi(p^e) = p^e - p^{e-1}$ für $e \geq 1$.*

Beweis: Es gibt genau p^{e-1} Zahlen, die kleiner oder gleich p^e sind, und die durch p teilbar sind.

Umformulierung: $\phi(p^e) = p^e(1 - \frac{1}{p})$. Demnach gilt

$$\boxed{\phi(n) = n \cdot \prod_{p|n} \big(1 - \frac{1}{p}\big).}$$