ulm university universität **uulm**

Skript zur Vorlesung

Anwendungen der Zahlentheorie in der Kombinatorik

Sommersemester 2014

Prof. Dr. Helmut Maier
Hans- Peter Reck

Institut für Zahlentheorie und Wahrscheinlichkeitstheorie
Universität Ulm

Inhaltsverzeichnis

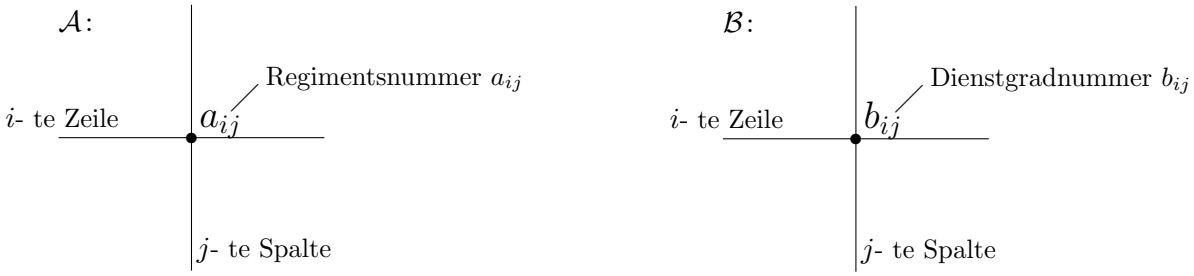
Kapitel 1

Orthogonale Lateinische Quadrate, affine und projektive Ebenen, endliche Körper

1.1 Einführung

Orthogonale Lateinische Quadrate treten vermutlich zum ersten Mal im Eulerschen Offiziersproblem (Euler, 1782) auf.
Demnach entstammen 36 Offiziere sechs Regimentern, sechs aus jedem Regiment. Von jedem Regiment ist jeder der sechs Dienstgrade genau einmal vertreten. Die Offiziere sollen nun so in einem Quadrat antreten, dass in jeder Zeile und in jeder Spalte sowohl jedes Regiment als auch jeder Dienstgrad genau einmal vertreten ist.

Zur Analyse dieser Frage numerieren wir sowohl die Regimenter als auch die Dienstgrade mit 1 bis 6 durch und stellen uns eine Lösung des beschriebenen Problems vor.
Wir betrachten zwei Matrizen $\mathcal{A}$ und $\mathcal{B}$. Die i- te Zeile und j- te Spalte von $\mathcal{A}$ enthalte die Regimentsnummer, die i- te Zeile und j- te Spalte von $\mathcal{B}$ die Nummer des Dienstgrades des dort stehenden Offiziers:



Welche Eigenschaften müssen die Matrizen $\mathcal{A}$ und $\mathcal{B}$ besitzen?

Jedes Regiment, also jede Zahl von 1 bis 6, soll in einer gegebenen Zeile bzw. Spalte genau einmal vertreten sein, d.h. $\mathcal{A}$ muss ein sogenanntes Lateinisches Quadrat sein.
Dasselbe gilt für die Dienstgrade und damit für $\mathcal{B}$.

Definition 1.1.1. Eine Matrix vom Typ (n, n), deren Elemente einer Menge von n Symbolen entnommen sind, heißt Lateinisches Quadrat der Ordnung n, falls in jeder Zeile und in jeder Spalte jedes Symbol genau einmal vertreten ist.

Definition 1.1.2. Unter dem Hadamard- Produkt zweier Matrizen $\mathcal{A} = (a_{ij})$ und $\mathcal{B} = (b_{ij})$ vom Typ (n, n) versteht man $\mathcal{C} = (a_{ij}, b_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}}$.

Beispiel 1.1.1. Es seien die Matrizen

$$\mathcal{A} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{pmatrix} \quad \text{und} \quad \mathcal{B} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{pmatrix}$$

gegeben. Dann ist

$$\mathcal{C} = \begin{pmatrix} (1,1) & (2,2) & (3,3) \\ (2,3) & (3,1) & (1,2) \\ (3,2) & (1,3) & (2,1) \end{pmatrix}.$$

Definition 1.1.3. Zwei Lateinische Quadrate $\mathcal{A}$ und $\mathcal{B}$ heißen orthogonal, wenn in ihrem Hadamard-Produkt jedes der n^2 möglichen Paare genau einmal vorkommt.

Das Eulersche Offiziersproblem lässt sich nun so formulieren:
Konstruiere zwei orthogonale Lateinische Quadrate der Ordnung 6.

Wie schon Euler vermutete, besitzt jedoch das Existenzproblem für orthogonale Lateinische Quadrate der Ordnung 6 keine Lösung. Das Eulersche Offiziersproblem ist somit unlösbar.

Das Konzept der orthogonalen Lateinischen Quadrate hat in neuerer Zeit in der Planung von Experimenten praktische Bedeutung gewonnen. Dieses Konzept wurde zuerst von dem Statistiker Ronald Fischer eingeführt. Das Prinzip soll anhand eines Beispieles angedeutet werden:
Davies (The Application of Variance Analysis to some Problems of Petroleum Technology, Technical Paper, Institute of Petroleum, London, 1945) hat orthogonale Lateinische Quadrate der Ordnung 7 zum Test von sieben Benzinsorten benützt.
Zum Test wurde ein Auto verwendet, das in jedem Experiment über eine feste Versuchsstrecke von 20 Meilen gefahren wurde.
Es ergeben sich nun folgende Probleme:
Die Beurteilung der Qualität eines Benzintyps kann stark von den Verkehrsbedingungen und der Fahrweise abhängen. Die Fahrweise eines Fahrers wiederum wird durch die Verkehrsbedingungen und andere Faktoren wie Tageszeit usw. beeinflusst.
Um derartige Abhängigkeiten weitgehend auszuschalten, werden an das Experiment folgende Forderungen gestellt: Das Auto wird 49mal gefahren. Es werden dabei sieben Fahrer verwendet. Jeder fährt das Auto siebenmal. Jeder der sieben Fahrer soll jeden der sieben Benzintypen einmal benützen. Jeder der sieben Fahrer soll an jedem der sieben Wochentagen und in jeder Tagesperiode genau einmal fahren.

Der Plan des Experiments wird durch eine $(7, 7)$- Matrix ausgegeben, deren Zeilenindex den Wochentag und deren Spaltenindex die Tageszeit angibt. Die Einträge geben das Paar (Fahrer, Benzintyp) wieder, mit dem die Fahrt durchgeführt wird.

Diese Matrix wird nun aus einem Paar von orthogonalen Lateinischen Quadraten der Ordnung 7 konstruiert.

$$\mathcal{A} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 5 & 6 & 7 & 1 \\ 3 & 4 & 5 & 6 & 7 & 1 & 2 \\ 4 & 5 & 6 & 7 & 1 & 2 & 3 \\ 5 & 6 & 7 & 1 & 2 & 3 & 4 \\ 6 & 7 & 1 & 2 & 3 & 4 & 5 \\ 7 & 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} \quad \text{und} \quad \mathcal{B} = \begin{pmatrix} 2 & 4 & 6 & 1 & 3 & 5 & 7 \\ 3 & 5 & 7 & 2 & 4 & 6 & 1 \\ 4 & 6 & 1 & 3 & 5 & 7 & 2 \\ 5 & 7 & 2 & 4 & 6 & 1 & 3 \\ 6 & 1 & 3 & 5 & 7 & 2 & 4 \\ 7 & 2 & 4 & 6 & 1 & 3 & 5 \\ 1 & 3 & 5 & 7 & 2 & 4 & 6 \end{pmatrix}$$

1.2 Designs

Definition 1.2.1. Ein balanciertes unvollständiges (Block)- Design (BIBD) mit den Parametern (v, b, r, k, λ), also kurz ein Design $D(v, b, r, k, \lambda)$, ist ein Paar $(\mathcal{D}, \mathcal{B})$, wobei $\mathcal{D}$ eine Menge von v Objekten und $\mathcal{B}$ eine Menge von b Teilmengen von $\mathcal{D}$ ist, die Blöcke genannt werden, so dass jeder Block genau k verschiedene Objekte enthält, jedes Objekt in genau r verschiedenen Blöcken vorkommt und jedes Paar von verschiedenen Objekten $\{a_i, a_j\}$ zusammen in genau λ Blöcken vorkommt.

Beispiel 1.2.1. Es sei $\mathcal{D} = \{1, 2, \ldots, 7\}$ und $\mathcal{B} = \{B_1, \ldots, B_7\}$ mit den Blöcken

$$\begin{aligned} B_1 &= \{3,5,6,7\}, \quad B_2 = \{1,4,6,7\}, \quad B_3 = \{1,2,5,7\}, \quad B_4 = \{1,2,3,6\}, \\ B_5 &= \{2,3,4,7\}, \quad B_6 = \{1,3,4,5\}, \quad B_7 = \{2,4,5,6\}. \end{aligned}$$

Wie man nachprüfen kann, tritt jedes Objekt in genau vier Blöcken auf und jedes Paar von Objekten in genau zwei Blöcken. Also ist $(\mathcal{D}, \mathcal{B})$ ein Design $D(7, 7, 4, 4, 2)$.

Satz 1.2.1. *Für ein Design $D(v, b, r, k, \lambda)$ gilt:*

$$\begin{aligned} b \cdot k &= v \cdot r \quad \textit{und} \\ r \cdot (k-1) &= \lambda \cdot (v-1). \end{aligned}$$

Beweis. Wir zählen die Menge $\mathcal{M}_1 = \{(P, \mathcal{B})\colon P \in \mathcal{D}, B \in \mathcal{B}, P \in B\}$ auf zwei Arten ab. Da jeder Block k Objekte enthält, ist $|\mathcal{M}_1| = b \cdot k$. Da jeder Punkt in r Blöcken vorkommt, ist $|\mathcal{M}_1| = v \cdot r$.

Nun wird die Menge $\mathcal{M}_2 = \{(P_1, P_2, \mathcal{B})\colon P_1 \neq P_2 \in \mathcal{D}, B \in \mathcal{B}, P_1, P_2 \in B\}$ auf zwei Arten abgezählt. Zu jedem $P_1 \in \mathcal{D}$ gibt es r Blöcke mit $P_1 \in B$. Diese enthalten zusammen $r \cdot (k-1)$ Objekte $P_1 \neq P_2$. Also ist $|\mathcal{M}_2| = v \cdot r \cdot (k-1)$. Da andererseits jedes von den $v \cdot (v-1)$ Paaren (P_1, P_2) jeweils in λ Blöcken enthalten ist, gilt: $|\mathcal{M}_2| = \lambda \cdot v \cdot (v-1)$. □

1.3 Affine und projektive Ebenen

Der allgemeine Begriff der (endlichen oder unendlichen) affinen Ebene stellt eine Verallgemeinerung der in der Linearen Algebra betrachteten Ebenen

$$K^2 = \{\vec{x} = (x, y)\colon x, y \in K\},$$

wobei K ein Körper ist, dar.
Die Elemente $\vec{x} = (x, y)$ von K^2 heißen Punkte der affinen Ebene, Teilmengen g der Form

$$g = \{\vec{x}_0 + t \cdot \vec{y}\colon t \in K\}$$

mit $\vec{y} \neq \vec{0}$ heißen Geraden.
Die affine Ebene K^2 ist endlich bzw. unendlich, wenn der Körper K endlich bzw. unendlich ist.

Während in der Analysis die unendlichen affinen Ebenen über den Körpern $\mathbb{R}$ oder $\mathbb{C}$ die Hauptrolle spielen, tun dies in der Kombinatorik die endlichen affinen Ebenen über endlichen Körpern.
Mit Methoden der Linearen Algebra beweist man leicht folgende Tatsachen über die affine Ebene $\mathbb{E} = K^2$.

- A1:
  Zu je zwei verschiedenen Punkten P_1, P_2 von $\mathbb{E}$ gibt es genau eine Gerade g, so dass $P_1, P_2 \in g$.

- A2:
  Ist g_1 eine Gerade, P ein Punkt mit $P \notin g_1$, so gibt es genau eine Gerade g_2 mit $P \in g_2$ und $g_2 \cap g_1 = \emptyset$, die Parallele zu g_1 durch P.

- A3:
  Zwei Geraden schneiden sich stets in keinem oder in einem Punkt.

- A4:
  Die affine Ebene $\mathbb{E}$ enthält vier Punkte, von denen keine drei auf einer Geraden liegen.

Eine affine Ebene kann nun auch definiert werden, ohne einen Körper zugrunde zu legen:

Definition 1.3.1. Eine affine Ebene ist ein Paar $(\mathbb{E}, \mathbb{G})$ bestehend aus einer Menge $\mathbb{E}$, deren Elemente Punkte genannt werden, und einer Menge $\mathbb{G}$ von Teilmengen von $\mathbb{E}$, Geraden genannt, so dass die Axiome A1 bis A4 erfüllt sind.
Aus jeder affinen Ebene $(\mathbb{E}, \mathbb{G})$ kann nun eine Struktur mit einer einfacheren Axiomatik, eine sogenannte projektive Ebene, konstruiert werden. Man sieht leicht, dass die Parallelität eine Äquivalenzrelation auf der Menge $\mathbb{G}$ und somit eine Partition von $\mathbb{G}$ in Äquivalenzklassen, Parallelscharen genannt, ergibt.

Es sei eine affine Ebene $(\mathbb{E}, \mathbb{G})$ gegeben. Wir vergrößern $\mathbb{E}$, die Menge der Punkte, durch Hinzunahme der Menge $\mathcal{U}$ der Parallelscharen, unendlich ferne Punkte genannt. Ein unendlich ferner Punkt Q liegt genau dann auf einer Geraden g, wenn $g \in Q$, d.h. wenn g der Parallelenschar Q angehört.
Zu den Geraden von $\mathbb{G}$ fügen wir die unendlich ferne Gerade $\mathcal{U}$, die Menge aller unendlich fernen Punkte hinzu.
Das Paar $(\mathbb{P}, \mathbb{G}')$ mit $\mathbb{P} = \mathbb{E} \cup \mathcal{U}$ und $\mathbb{G}' = \mathbb{G} \cup \{\mathcal{U}\}$ erfüllt dann folgendes System von Axiomen:

- P1:
  Zu je zwei verschiedenen Punkten P_1, P_2 von $\mathbb{P}$ gibt es genau eine Gerade $g \in \mathbb{G}'$, so dass $P_1, P_2 \in g$.

- P2:
  Zwei verschiedene Geraden schneiden sich stets in genau einem Punkt.

- P3:
  Es enthält $\mathbb{P}$ vier Punkte, von denen keine drei auf einer Geraden liegen.

Definition 1.3.2. Eine projektive Ebene ist ein Paar $(\mathbb{P}, \mathbb{G}')$ bestehend aus einer Menge $\mathbb{P}$, deren Elemente Punkte genannt werden, und einer Menge $\mathbb{G}'$ von Teilmengen von $\mathbb{P}$, Geraden genannt, so dass die Axiome P1 bis P3 erfüllt sind. Ist $(\mathbb{E}, \mathbb{G}) = (K^2, \mathbb{G})$ eine affine Ebene über einem Körper K, so können die Punkte der durch Erweiterung von $\mathbb{E}$ entstehenden projektiven Ebene $\mathbb{P}$ durch homogene Koordinaten beschrieben werden.

Wir identifizieren dazu mittels der Abbildung $\Phi\colon \mathbb{E} = K^2 \to K^3$ die Punkte von $\mathbb{E}$ mit Geraden in K^3 durch den Ursprung $(0,0,0)$. Die Abbildung Φ ist wie folgt definiert:
Ist $P = (x,y)$, so ist $\Phi(P)$ die Gerade durch den Ursprung $(0,0,0)$ und den Punkt $(x,y,1)$. Dieser Punkt gehört der Ebene $\mathbb{E}^* = \{(x,y,1)\colon x,y \in K\}$ an, die zur xy- Ebene parallel ist.
Das Paar $(\Phi(\mathbb{E}), \Phi(\mathbb{G}))$ ist dann eine affine Ebene, die zu $\mathbb{E}$ "isomorph" ist. Wie man leicht sieht, sind die Geraden in $\Phi(\mathbb{G})$ die Mengen, die aus den Geraden von festen Ebenen durch $(0,0,0)$ bestehen.
Es vermittelt Φ also Abbildungen zwischen folgenden Objekten:
P Punkt von $\mathbb{E} = K^2 \Rightarrow_\Phi$ $\Phi(P)$ (Punkt von $\Phi(\mathbb{E})$: Gerade durch $(0,0,0)$)
g Gerade von $\mathbb{E} = K^2 \Rightarrow_\Phi$ $\Phi(g)$ (Gerade von $\Phi(\mathbb{E})$: Menge von Geraden in einer Ebene durch $(0,0,0)$)

Wir ergänzen nun $\Phi(\mathbb{E})$ durch Hinzunahme der unendlich fernen Punkte und der unendlich fernen Geraden $\mathcal{U}$. Wir definieren als unendlich ferne Punkte die Geraden des K^3 durch $(0,0,0)$, welche die Ebene $\mathbb{E}^*$ nicht schneiden. Dies sind die Geraden, die in der xy- Ebene verlaufen, also die Geraden von der Form $g = \{(ux, uy, 0)\colon u \in K\}$. Wir fügen ferner die Menge $\mathcal{U}$ als neue Gerade, die unendlich ferne Gerade hinzu. Dann erfüllt das Paar $(\mathbb{P}, \mathbb{G}')$ mit $\mathbb{P} = \Phi(\mathbb{E}) \cup \mathcal{U}$ und $\mathbb{G}' = \Phi(\mathbb{G}) \cup \{\mathcal{U}\}$ die Axiome einer projektiven Ebene.
Die homogenen Koordinaten eines Punktes P von $\mathbb{P}$ ist die Menge aller von $(0,0,0)$ verschiedenen Punkte des K^3, die auf der Geraden $\Phi(P)$ liegen, also gerade die Menge $\{(ux, uy, u)\colon u \in K\backslash\{0\}\}$. Die homogenen Koordinaten sind somit nur bis auf den Proportionalitätsfaktor $u \neq 0$ bestimmt.

Satz 1.3.1. *Ist K ein endlicher Körper von q Elementen, so besteht die projektive Ebene $(\mathbb{P}, \mathbb{G})$ über K aus $q^2 + q + 1$ Punkten. Es gibt $q^2 + q + 1$ Geraden, von denen jede $(q+1)$ Punkte enthält. Durch jeden Punkt gehen $(q+1)$ Geraden. So ist $(\mathbb{P}, \mathbb{G})$ mit den Punkten als Objekten und den Geraden als Blöcken ein Design $D(q^2+q+1, q^2+q+1, q+1, q+1, 1)$.*

Bevor wir diesen Satz beweisen, betrachten wir zunächst den Fall einer allgemeinen endlichen projektiven Ebene, der kein Körper zugrunde liegen braucht.

Satz 1.3.2. *Es sei $(\mathbb{P}, \mathbb{G})$ eine endliche projektive Ebene. Dann gibt es eine natürliche Zahl $n \geq 2$, die Ordnung von $\mathbb{P}$ genannt, so dass folgendes gilt: $(\mathbb{P}, \mathbb{G})$ hat $n^2 + n + 1$ Punkte und $n^2 + n + 1$ Geraden. Jede Gerade enthält $(n+1)$ Punkte; durch jeden Punkt gehen $(n+1)$ Geraden. So ist $(\mathbb{P}, \mathbb{G})$ mit den Punkten als Objekten und den Geraden als Blöcken ein Design $D(n^2+n+1, n^2+n+1, n+1, n+1, 1)$.*

Beweis. Nach $P3$ gibt es vier Punkte P_1, P_2, Q_1, Q_2 in $(\mathbb{P}, \mathbb{G})$, von denen keine drei auf einer Geraden liegen. Es sei g_1 die Gerade durch P_1 und Q_1, weiter g_2 die Gerade durch P_2 und Q_2 sowie r die Anzahl der Geraden durch P_2. Jede dieser Geraden schneidet g_1 in genau einem Punkt. Umgekehrt gibt es zu jedem Punkt Q von g_1 genau eine Gerade durch P_2, die g_1 in Q schneidet, womit r Punkte auf g_1 liegen. Dies gilt auch für jede andere Gerade, die nicht durch P_2 geht. Da in unseren Überlegungen P_2 durch Q_2 ersetzt werden kann, enthält auch jede Gerade, die nicht durch Q_2 geht, genau r Punkte. Also haben alle Geraden außer möglicherweise g_2 genau r Punkte. Wir können in unseren Überlegungen das Tripel (g_2, P_2, Q_2) durch das Tripel (g_1, P_1, Q_1) ersetzen und erhalten, dass alle Geraden außer möglicherweise g_1 dieselbe Anzahl an Punkten enthalten. Da es aber mindestens sechs Geraden gibt, nämlich die Verbindungsgeraden der Punkte P_1, P_2, Q_1, Q_2, enthalten alle Geraden r Punkte.
Wir haben anfangs gezeigt, dass die Anzahl der Geraden durch P_2 gleich der Anzahl der Punkte auf g_1 ist. Da in dieser Überlegung das Paar (P_2, g_1) durch ein beliebiges Paar (P, g) mit $P \notin g$ ersetzt werden kann, gehen durch jeden Punkt r Geraden.
Wir setzen $n = r - 1$.
Es sei $P \in \mathbb{P}$ beliebig. Jeder Punkt von $\mathbb{P}\backslash\{P\}$ liegt auf genau einer der $n+1$ Geraden durch P. Jede dieser Geraden enthält genau n von P verschiedene Punkte. So enthält $\mathbb{P}$ insgesamt n^2+n+1 Punkte. Indem man in jeder der vorausgehenden Überlegungen die Begriffe "Punkt" und "Gerade" vertauscht (Dualitätsprinzip) erhält man, dass $\mathbb{P}$ auch $n^2 + n + 1$ Geraden enthält. □

Beweis. (Beweis von Satz 1.3.1:)
Der $K^3\backslash\{(0,0,0)\}$ enthält q^3-1 Elemente. Je $(q-1)$ dieser Elemente gehören zu derselben Geraden durch den Ursprung, also zum selben Punkt der projektiven Ebene.
Damit enthält $\mathbb{P}$ somit $\frac{q^3-1}{q-1} = q^2+q+1$ Punkte. Der Rest der Behauptung folgt aus Satz 1.3.2. $\square$

Beispiel 1.3.1. Es sei $K = \{0,1\}$ der Körper mit zwei Elementen. Dann liegt auf jeder Geraden durch $(0,0,0)$ genau ein Element aus $K^3\backslash\{(0,0,0)\}$.
Daher ist

$$\begin{aligned}\mathbb{P} &= \{\{(0,0,1)\},\{(0,1,0)\},\{(0,1,1)\},\{(1,0,0)\},\{(1,0,1)\},\{(1,1,0)\},\{(1,1,1)\}\}\\ &:= \{P_1,P_2,P_3,P_4,P_5,P_6,P_7\}.\end{aligned}$$

Liegen zwei Punkte auf einer Geraden, so liegt auch jeder der durch eine beliebige Linearkombination der homogenen Koordinaten dieser zwei Punkte dargestellte Punkt darauf. $\mathbb{P}$ hat damit folgende Geraden:

$$\begin{aligned}g_1 &= \{P_1,P_2,P_3\},\ g_2=\{P_1,P_4,P_5\},\ g_3=\{P_1,P_6,P_7\}\\ g_4 &= \{P_2,P_4,P_6\},\ g_5=\{P_2,P_5,P_7\},\ g_6=\{P_3,P_5,P_6\}\\ g_7 &= \{P_3,P_4,P_7\}\end{aligned}$$

Beispiel 1.3.2. Wir haben $K = \{0,1,-1\}$ mit den Verknüpfungstafeln

+	0	1	-1
0	0	1	-1
1	1	-1	0
-1	-1	0	1

und

·	1	-1
1	1	-1
-1	-1	1

Wir listen zunächst die homogenen Koordinaten der dreizehn Punkte auf:

$$\begin{aligned}P_1 &: \{(0,0,1),(0,0,-1)\},\quad P_2:\{(0,1,0),(0,-1,0)\},\quad P_3:\{(0,1,1),(0,-1,-1)\}\\ P_4 &: \{(0,-1,1),(0,1,-1)\},\quad P_5:\{(1,0,0),(-1,0,0)\},\quad P_6:\{(1,0,1),(-1,0,-1)\}\\ P_7 &: \{(1,0,-1),(-1,0,1)\},\quad P_8:\{(1,1,0),(-1,-1,0)\},\quad P_9:\{(1,-1,0),(-1,1,0)\}\\ P_{10} &: \{(1,1,1),(-1,-1,-1)\},\quad P_{11}:\{(1,1,-1),(-1,-1,1)\},\quad P_{12}:\{(1,-1,1),(-1,1,-1)\}\\ P_{13} &: \{(1,-1,-1),(-1,1,1)\}.\end{aligned}$$

Die Geraden sind gegeben durch:

$$\begin{aligned}g_1 &= \{P_1,P_2,P_3,P_4\},\ g_2=\{P_1,P_5,P_6,P_7\},\ g_3=\{P_1,P_8,P_{10},P_{11}\}\\ g_4 &= \{P_1,P_9,P_{12},P_{13}\},\ g_5=\{P_2,P_5,P_8,P_9\},\ g_6=\{P_2,P_6,P_{10},P_{12}\}\\ g_7 &= \{P_2,P_7,P_{11},P_{13}\},\ g_8=\{P_3,P_5,P_{10},P_{13}\},\ g_9=\{P_3,P_6,P_9,P_{11}\}\\ g_{10} &= \{P_3,P_7,P_8,P_{12}\},\ g_{11}=\{P_4,P_5,P_{11},P_{12}\},\ g_{12}=\{P_4,P_6,P_8,P_{13}\}\\ g_{13} &= \{P_4,P_7,P_9,P_{10}\}.\end{aligned}$$

Beispiel 1.3.3. (Projektive Ebene der Ordnung 4):
Diese wird mittels des Körpers $K = \mathbb{F}_4$ konstruiert. Es ist $\mathbb{F}_4 = \{0,1,t,t+1\}$. Die Rechenoperationen in $\mathbb{F}_4$ ergeben sich aus den beiden Grundregeln $1+1=0$ und $t^2 = t\cdot t = t+1$.

Daraus ergeben sich folgende Additions- und Multiplikationstafeln (mittels der Assoziativ- und Distributivgesetze):

$+$	0	1	t	$t+1$
0	0	1	t	$t+1$
1	1	0	$t+1$	t
t	t	$t+1$	0	1
$t+1$	$t+1$	t	1	0

und

$\cdot$	1	t	$t+1$
1	1	t	$t+1$
t	t	$t+1$	t
$t+1$	$t+1$	t	1

Dabei ist 0 das neutrale Element der Addition und 1 das der Multiplikation, und es gilt $0 \cdot a = a \cdot 0 = 0$ für alle $a \in \mathbb{F}_4$.

Wir geben nun die homogenen Koordinaten der 21 Punkte von $\mathbb{P}(\mathbb{F}_4)$ an:

$$
\begin{array}{ll}
P_1 : \{(0,0,1),(0,0,t),(0,0,t+1)\}, & P_2 : \{(0,1,0),(0,t,0),(0,t+1,0)\} \\
P_3 : \{(0,1,1),(0,t,t),(0,t+1,t+1)\}, & P_4 : \{(0,1,t),(0,t,t+1),(0,t+1,1)\} \\
P_5 : \{(0,1,t+1),(0,t,1),(0,t+1,t)\}, & P_6 : \{(1,0,0),(t,0,0),(t+1,0,0)\} \\
P_7 : \{(1,0,1),(t,0,t),(t+1,0,t+1)\}, & P_8 : \{(1,0,t),(t,0,t+1),(t+1,0,1)\} \\
P_9 : \{(1,0,t+1),(t,0,1),(t+1,0,t)\}, & P_{10} : \{(1,1,0),(t,t,0),(t+1,t+1,0)\} \\
P_{11} : \{(1,1,1),(t,t,t),(t+1,t+1,t+1)\}, & P_{12} : \{(1,1,t),(t,t,t+1),(t+1,t+1,1)\} \\
P_{13} : \{(1,1,t+1),(t,t,1),(t+1,t+1,t)\}, & P_{14} : \{(1,t,0),(t,t+1,0),(t+1,1,0)\} \\
P_{15} : \{(1,t,1),(t,t+1,t),(t+1,1,t+1)\}, & P_{16} : \{(1,t,t),(t,t+1,t+1),(t+1,1,1)\} \\
P_{17} : \{(1,t,t+1),(t,t+1,1),(t+1,1,t)\}, & P_{18} : \{(1,t+1,0),(t,1,0),(t+1,t,0)\} \\
P_{19} : \{(1,t+1,1),(t,1,t),(t+1,t,t+1)\}, & P_{20} : \{(1,t+1,t),(t,1,t+1),(t+1,t,1)\} \\
P_{21} : \{(1,t+1,t+1),(t,1,1),(t+1,t,t)\}. &
\end{array}
$$

und die ersten 14 der 21 Geraden:

$$
\begin{array}{ll}
g_1 = \{P_1,P_2,P_3,P_4,P_5\}, & g_2 = \{P_1,P_6,P_7,P_8,P_9\} \\
g_3 = \{P_1,P_{10},P_{11},P_{12},P_{13}\}, & g_4 = \{P_1,P_{14},P_{15},P_{16},P_{17}\} \\
g_5 = \{P_1,P_{18},P_{19},P_{20},P_{21}\}, & g_6 = \{P_2,P_6,P_{10},P_{14},P_{18}\} \\
g_7 = \{P_2,P_7,P_{11},P_{15},P_{19}\}, & g_8 = \{P_2,P_8,P_{12},P_{16},P_{20}\} \\
g_9 = \{P_2,P_9,P_{13},P_{17},P_{21}\}, & g_{10} = \{P_3,P_6,P_{11},P_{16},P_{21}\} \\
g_{11} = \{P_3,P_7,P_{10},P_{17},P_{20}\}, & g_{12} = \{P_3,P_8,P_{13},P_{14},P_{19}\} \\
g_{13} = \{P_3,P_9,P_{12},P_{15},P_{18}\}, & g_{14} = \{P_4,P_6,P_{12},P_{17},P_{19}\}.
\end{array}
$$

Die Bestimmung der restlichen sieben Geraden ist Übungsaufgabe.

1.4 Projektive Ebenen und Orthogonale Lateinische Quadrate

Definition 1.4.1. Für $n \in \mathbb{N}$ und $n \geq 2$ sei $N(n)$ die maximale Anzahl von paarweise orthogonalen Lateinischen Quadraten (OLQ) der Ordnung n.

Satz 1.4.1. *Es ist*

$$N(n) \leq n - 1.$$

Beweis. Es sei $\mathcal{M}$ eine Menge von l OLQ

$$\mathcal{A}^{(1)} = (a_{ij}^{(1)})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}}, \ldots, \mathcal{A}^{(l)} = (a_{ij}^{(l)})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}}$$

der Ordnung n.

Die Änderung der Namen der Elemente in einem einzelnen Quadrat $\mathcal{A}^{(k)}$ ändert nichts an der Orthogonalität. Somit können wir annehmen, dass die ersten Zeilen in allen $\mathcal{A}^{(k)}$ die Form $(1, 2, \ldots, n)$ haben. Im Hadamard- Produkt zweier $\mathcal{A}^{(k)}$ kommen daher die Paare $(1, 1), \ldots, (n, n)$ alle genau einmal in der ersten Zeile vor. Die Elemente $a_{21}^{(k)}$ müssen somit alle untereinander verschieden und auch von 1 verschieden sein. Daher ist $l \leq n - 1$. □

Es stellt sich die Frage, für welche n die maximale Anzahl $N(n) = n-1$ von OLQ tatsächlich erreicht wird.
Der nächste Satz zeigt, dass dies äquivalent zur Existenz einer projektiven Ebene der Ordnung n ist.

Satz 1.4.2. *Es sei $n \geq 2$. Es gilt genau dann $N(n) = n-1$, wenn eine projektive Ebene der Ordnung n existiert.*

Beweis. Wir nehmen die Existenz einer projektiven Ebene der Ordnung n an und konstruieren hieraus eine Menge von $n-1$ orthogonalen Lateinischen Quadraten. Diese Konstruktion kann auch "umgekehrt" werden, womit sich beide Existenzaussagen als äquivalent erweisen.
Es sei $(\mathbb{P}, \mathbb{G})$ eine projektive Ebene der Ordnung n und L eine beliebige Gerade von $\mathbb{P}$. Nach Satz 1.3.2 enthält L genau $n+1$ Punkte, die wir als $U, V, W_1, \ldots W_{n-1}$ benennen. Durch jeden dieser Punkte gehen nach Satz 1.3.2 außer L noch n weitere Geraden. Die (jeweils von L verschiedenen) Geraden durch U seien $u_1, \ldots, u_n$, die durch V seien $v_1, \ldots, v_n$ und die durch W_k mit $1 \leq k \leq n-1$ seien $w_{k,1}, \ldots, w_{k,n}$.
Das k- te lateinische Quadrat $\mathcal{A}^{(k)} = (a_{ij}^{(k)})$ wird nun folgendermaßen konstruiert: Es gibt genau eine Gerade $w_{k,l}$ von den Geraden $w_{k,1}, \ldots, w_{k,n}$ durch W_k, die durch den Schnittpunkt von u_i und v_j geht. Wir setzen dann: $\mathcal{A}_{ij}^{(k)} = l$.
Die paarweise Orthogonalität der so konstruieren $\mathcal{A}^{(k)}$ folgt leicht aus den Eigenschaften von $(\mathbb{P}, \mathbb{G})$. □

1.5 Möbiussche Umkehrformel, endliche Körper

Definition 1.5.1. Eine arithmetische (oder auch eine zahlentheoretische) Funktion ist eine Abbildung $f\colon \mathbb{N} \to \mathbb{C}$ von den natürlichen Zahlen in die komplexen Zahlen. Eine arithmetische Funktion f heißt additiv, falls $f(mn) = f(m) + f(n)$ für $ggT(m, n) = 1$ ist bzw. multiplikativ, falls $f(1) = 1$ und $f(mn) = f(m)f(n)$ für $ggT(m, n) = 1$ ist. Sie heißt vollständig additiv bzw. vollständig multiplikativ, falls die Gleichungen $f(mn) = f(m) + f(n)$ bzw. $f(mn) = f(m)f(n)$ auch ohne die Zusatzbedingung $ggT(m, n) = 1$ gelten.

Im folgenden werden einige Beispiele arithmetischer Funktionen definiert:

Definition 1.5.2. 1. Die Funktion

$$\epsilon(n) = \begin{cases} 1, & \text{falls} \quad n = 1, \\ 0, & \text{sonst} \end{cases}$$

ist vollständig multiplikativ.

2. Es sei $\Omega(n) := \sum_{p^\alpha | n} \alpha$ die Anzahl der verschiedenen Primfaktoren von n (mit Vielfachheit gezählt) und $\nu(n) := \sum_{p|n} 1$ die Anzahl der verschiedenen Primfaktoren von n. Dann ist Ω vollständig additiv und ν additiv.

3. Die Möbiusfunktion μ ist durch

$$\mu(n) = \begin{cases} (-1)^{\nu(n)}, & \text{falls } n \text{ quadratfrei ist,} \\ 0 & \text{sonst} \end{cases}$$

definiert. Wir werden zeigen, dass μ multiplikativ ist.

4. Die Teilerfunktion $\tau(n) := \sum_{d|n} 1$, die Anzahl der (positiven) Teiler von n, ist, wie wir zeigen werden, multiplikativ.

Definition 1.5.3. Es seien f und g arithmetische Funktionen. Unter der Faltung $f \star g$ von f und g versteht man die arithmetische Funktion

$$(f \star g)(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right).$$

Unter der Summe $f + g$ von f und g versteht man die arithmetische Funktion

$$(f + g)(n) = f(n) + g(n).$$

Beispiel 1.5.1. Es ist $\tau(n) = \sum_{d|n} 1 = \sum_{d|n} 1(d) \cdot 1(\frac{n}{d})$, also $\tau = 1 \star 1$.

Satz 1.5.1. *Die Menge A aller arithmetischen Funktionen bildet mit der Addition und der Faltung als Multiplikation einen kommutativen Ring mit Einselelement ϵ.*

Beweis. Die Menge A bildet offenbar unter der Addition von Funktionen eine abelsche Gruppe. Das Distributivgesetz $f \star (g + h) = (f \star g) + (f \star h)$ ist klar.
Es bleibt die Kommutativität und Assoziativität der Faltung zu zeigen, sowie dass ϵ Einselement ist:

- Es ist $(f \star g)(n) = \sum_{d|n} f(d) g(\frac{n}{d})$. Durchläuft d alle Teiler von n, so auch $d' = \frac{n}{d}$. Also ist

$$(f \star g)(n) = \sum_{d'|n} f\left(\frac{n}{d'}\right) g(d') = (g \star f)(n).$$

- Es seien f, g, h arithmetische Funktionen. Dann ist

$$\begin{aligned} ((f \star g) \star h)(n) &= \sum_{d|n} (f \star g)(d) \cdot h\left(\frac{n}{d}\right) \\ &= \sum_{d|n} \sum_{d_1|d} f(d_1) g\left(\frac{d}{d_1}\right) h\left(\frac{n}{d}\right) \\ &\underset{d=d_1 d_2, \frac{n}{d}=d_3}{=} \sum_{\substack{d_1,d_2,d_3 \\ d_1 d_2 d_3 = n}} f(d_1) g(d_2) h(d_3). \end{aligned}$$

  Derselbe Ausdruck ergibt sich für $(f \star (g \star h))(n)$. Also ist $(f \star g) \star h) = f \star (g \star h)$.

- Es ist $(\epsilon \star g)(n) = \sum_{d|n} \epsilon(d) f(\frac{n}{d}) = \epsilon(1) f(n) = f(n)$. Also ist $\epsilon \star f = f$.

□

Satz 1.5.2. *Die Faltung zweier multiplikativer Funktionen ist multiplikativ.*

Beweis. Es seien $f, g \in A$ multiplikativ und $F = f \star g$. Weiter sei $ggT(m,n) = 1$. Dann ist

$$F(mn) = \sum_{\substack{d_1,d_2 \\ d_1 d_2 = mn}} f(d_1)g(d_2).$$

Wir schreiben $d_1 = e_1e_2$ mit $e_1 = ggT(d_1, m)$ und $e_2 = ggT(d_1, n)$ sowie $d_2 = e_3e_4$ mit $e_3 = ggT(d_2, m)$ und $e_4 = ggT(d_2, n)$. Dies ist bei gegebenem d_1 und d_2 auf genau eine Art möglich. Dann ist $e_1e_3 = m$ und $e_2e_4 = n$.
Also ist wegen der Multiplikativität von f und g

$$\begin{aligned} F(mn) &= \sum_{\substack{e_1,e_2,e_3,e_4 \\ e_1e_3=m, e_2e_4=n}} f(e_1e_2)g(e_3e_4) = \sum_{\substack{e_1,e_2,e_3,e_4 \\ e_1e_3=m, e_2e_4=n}} f(e_1)f(e_2)g(e_3)g(e_4) \\ &= \sum_{\substack{e_1,e_3 \\ e_1e_3=m}} f(e_1)g(e_3) \sum_{\substack{e_2,e_4 \\ e_2e_4=n}} f(e_2)g(e_4) = F(m) \cdot F(n). \end{aligned}$$

□

Satz 1.5.3. *Die Teilerfunktion ist multiplikativ.*

Beweis. Aus Satz 1.5.2 ergibt sich mit $\tau = 1 \star 1$ ein Beweis für die Multiplikativität der Teilerfunktion. □

Beispiel 1.5.2. Es sei $\sigma_k(n) := \sum_{d|n} d^k$. Es ist $\sigma_k = f \star 1$ mit $f(n) = n^k$: Nach Satz 1.5.2 ist σ_k multiplikativ.

Satz 1.5.4. *Es ist $\mu \star 1 = \epsilon$.*

Beweis. Nach Satz 1.5.2 ist $\mu \star 1$ multiplikativ. Es bleibt, die Werte von $\mu \star 1$ für Primzahlpotenzen zu bestimmen: Für $\alpha \geq 1$ ist

$$(\mu \star 1)(p^\alpha) = \sum_{\beta=0}^{\alpha} \mu\left(p^\beta\right) = 1 + \mu(p) = 0.$$

Also ist $\mu \star 1 = \epsilon$. □

Satz 1.5.5. *(Möbiussche Umkehrformel)*
Es seien f und g arithmetische Funktionen. Die folgenden Beziehungen sind äquivalent:

1. $F(n) = \sum_{d|n} f(d)$ *für alle* $n \in \mathbb{N}$
2. $f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right)$ *für alle* $n \in \mathbb{N}$.

Beweis. "⇒":
Nach der Definition der Faltung haben wir $F = 1 \star f$. Daraus folgt nach den Sätzen 1.5.1 und 1.5.3

$$\mu \star F = \mu \star (1 \star f) = (\mu \star 1) \star f = \epsilon \star f = f.$$

Also ist $\sum_{d|n} \mu(d) F(\frac{n}{d}) = f(n)$.

"$\Leftarrow$":
Es ist also $\mu \star F = f$. Dann ist

$$f \star 1 = 1 \star (\mu \star F) = (1 \star \mu) \star F = \epsilon \star F = F,$$

also $\sum_{d|n} f(d) = F(n)$. □

Wir kommen nun zur Konstruktion endlicher Körper. Die einfachsten sind die von Primzahlordnung.

Satz 1.5.6. *Es sei p eine Primzahl. Dann ist der Restklassenring $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ ein Körper mit p Elementen.*

Beweis. Die Existenz und Eindeutigkeit des multiplikativen Inversen ergibt sich aus der Tatsache der elementaren Zahlentheorie, dass die Kongruenz $ax \equiv 1 \bmod p$ für $a \not\equiv 0 \bmod p$ genau eine Lösung modulo p hat. Alle anderen Körpereigenschaften sind unmittelbar klar. □

Die Körper der Ordnung p^n mit einer Primzahl p und $n \in \mathbb{N}$ mit $n \geq 2$ werden nun als Restklassenringe des Polynomrings $(\mathbb{Z}/p\mathbb{Z})[x]$ konstruiert.

Definition 1.5.4. Unter einem Polynomring $K[x]$ über einem Körper K versteht man

$$K[x] := \left\{ f(x) = \sum_{\nu=0}^{n} a_\nu x^\nu \colon a_\nu \in K,\ \nu = 0, \ldots, n \in \mathbb{N}_0 \right\}.$$

Definition 1.5.5. Ein Element $f(x) = \sum_{\nu=0}^{n} a_\nu x^\nu \in K[x]$ heißt normiert, falls $a_n = 1$ ist. Weiter heißt f irreduzibel, falls $f \neq 0$ und $f \neq g \cdot h$ für alle $g, h \in K[x]$ mit $\deg g \geq 1$ und $\deg h \geq 1$ gilt.

Satz 1.5.7. *(Division mit Rest)*
Es sei $g \in K[x]$ und $g \neq 0$. Dann existieren zu jedem $f \in K[x]$ eindeutig bestimmte $q, r \in K[x]$ mit $f = q \cdot g + r$ mit $\deg r < \deg g$.

Beweis. Der Beweis folgt mittels der aus der Analysis bekannten "langen Division". □

Satz 1.5.8. *(Euklidischer Algorithmus)*
Es sei $f, g \in K[x]$ mit $g \neq 0$ und $\deg g < \deg f$. Dann existieren $s, t \in K[x]$ mit $fs + gt = 1$.

Beweis. Der Euklidische Algorithmus besteht aus einer wiederholten Anwendung der Division mit Rest (Satz 1.5.7).

$$\begin{cases} f = q_0 \cdot g + r_0 & \text{mit} \quad \deg r_0 < \deg g \ (r_0 \neq 0) \\ g = q_1 \cdot r_0 + r_1 & \text{mit} \quad \deg r_1 < \deg r_0 \ (r_1 \neq 0) \\ r_0 = q_2 \cdot r_1 + r_2 & \text{mit} \quad \deg r_2 < \deg r_1 \ (r_2 \neq 0) \\ \vdots & \\ r_{n-2} = q_n \cdot r_{n-1} + r_n & \text{mit} \quad \deg r_n < \deg r_{n-1} \ (r_n \neq 0) \\ r_{n-1} = q_{n+1} \cdot r_n. & \end{cases}$$

Dieses Schema tritt auch beim Euklidischen Algorithmus in der elementaren Zahlentheorie auf. Wie dort beweist man die Existenz von s und t, so dass $fs + gt = 1$ gilt. □

Satz 1.5.9. *Es seien $f, g, h \in K[x]$, wobei f und h teilerfremd seien. Weiter gelte $f|(gh)$. Dann folgt $f|g$.*

Beweis. Nach Satz 1.5.8 gibt es $s, t \in K[x]$ mit $hs + ft = 1$. Daraus folgt $f|(ghs + gft) = g$. □

Satz 1.5.10. *(Eindeutigkeit der Primfaktorzerlegung)*
Es sei $f \in K[x]$ normiert mit $\deg f = n \in \mathbb{N}_0$. Dann existieren bis auf die Reihenfolge eindeutige, normierte, irreduzible $f_{kl} \in K[x]$ mit

$$f = \prod_{k=1}^{n} \prod_{l=1}^{r_k} f_{kl} \qquad (*)$$

mit $\deg f_{kl} = k$ und $r_k \geq 0$ sowie $r_1 + 2r_2 + \ldots + nr_n = n$.

Beweis. Existenz:
Die Existenz beweisen wir mittels Induktion nach $n = \deg f$:
$n = 0$:
Dann ist $f = 1$ und die Behauptung $(*)$ gilt mit dem leeren Produkt.
$n \to n + 1$:
1. Fall: f ist irreduzibel: Dann gilt $(*)$ mit $n = 1$, $r_k = 1$ und $f_{11} = f$.
2. Fall: f ist reduzibel: Dann ist $f = g\dot{h}$ mit $1 \leq \deg f, \deg g < n$. Nach Induktionshypothese gilt die Behauptung für g und h und somit auch für f.
Eindeutigkeit:
Wir nehmen an, es gäbe ein f mit zwei verschiedenen Darstellungen

$$f = \prod_{\nu=1}^{m} g_\nu \quad \text{und} \quad f = \prod_{\mu=1}^{k} h_\mu.$$

Wir betrachten dasjenige Polynom, für das $\max\{m, k\}$ minimal ist. Aus $g_1 | h_1 \cdots h_k$ folgt $h_\nu = cg_1$ für ein ν. Damit ergibt sich

$$fg_1^{-1} = \prod_{\nu=2}^{m} g_\nu = c \cdot \prod_{\substack{\mu=1 \\ \mu \neq \nu}}^{r} h_\mu.$$

□

Satz 1.5.11. *(Existenz des irreduziblen Polynoms)*
Es sei K ein endlicher Körper mit $|K| = q$. Dann gilt: Die Anzahl $\pi_q(n)$ aller normierter und irreduzibler Polynome aus $K[x]$ vom Grade $n \in \mathbb{N}$ ist

$$\pi_q(n) = \frac{1}{n} \cdot \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d > 0.$$

Beweis. Jedes normierte Polynom $f \in K[x]$ hat die Form $f(x) = a_0 + a_1 x + \ldots + a_{n-1}x^{n-1} + x^n$. Für jedes $a_0, \ldots, a_{n-1}$ gibt es q Auswahlmöglichkeiten und somit gibt es q^n normierte Polynome vom Grad kleiner gleich n.
Nach Satz 1.5.10 besitzt jedes normierte Polynom f eine eindeutige Darstellung der Form

$$f = \prod_{k=1}^{n} \prod_{l=1}^{r_k} f_{kl}$$

mit $\deg f_{kl} = k$ und $r_k \geq 0$ sowie $r_1 + 2r_2 + \ldots + nr_n = n$ mit irreduziblem f_{kl}. Nach einem grundlegenden Anzahlproblem der Kombinatorik (Kombinationen mit Wiederholungen) gibt es

$$\binom{\pi_q(k) + r_k - 1}{r_k}$$

Möglichkeiten, r_k irreduzible Polynome aus $\pi_q(k)$ solchen Polynomen (möglicherweise mehrfach) auszuwählen.

Man stelle die Auswahl dar, indem man $\pi_q(k) + r_k - 1$ Zellen durch $\pi_q(k) - 1$ Striche markiert. Wir erhalten

$$q^n = \sum_{\substack{r_1+\ldots+nr_n=n \\ r_i \geq 0}} \prod_{k=1}^{n} \binom{\pi_q(k) + r_k - 1}{r_k}.$$

Diese Gleichungen werden mit Erzeugendenfunktionen behandelt. Wir benützen die Binomialreihe

$$(1-x)^{-\alpha} = \sum_{\nu=0}^{\infty} \binom{-\alpha}{\nu} (-1)^\nu x^\nu = \sum_{\nu=0}^{\infty} \binom{\alpha+\nu-1}{\nu} x^\nu$$

für $|x| < 1$. Dann folgt für $|x| < \frac{1}{4}$

$$\begin{aligned} \frac{1}{1-qx} &= 1 + \sum_{n=1}^{\infty} q^n x^n = 1 + \sum_{n=1}^{\infty} \sum_{r_1+\ldots+nr_n=n} \prod_{k=1}^{n} \binom{\pi_q(k) + r_k - 1}{r_k} x^k \\ &= \prod_{k=1}^{\infty} \left(\sum_{\nu=0}^{\infty} \binom{\pi_q(k) + \nu - 1}{\nu} x^{k\nu} \right) = \prod_{k=1}^{\infty} (1-x^k)^{-\pi_q(k)}. \end{aligned}$$

Mit der Logarithmusreihe

$$\log \frac{1}{1-x} = \sum_{n=1}^{\infty} \frac{x^n}{n}$$

für $|x| < 1$ folgt

$$\begin{aligned} \sum_{n=1}^{\infty} \frac{q^n}{n} \cdot x^n &= \log\left(\frac{1}{1-qx}\right) = \sum_{k=1}^{\infty} \pi_q(k) \log\left(\frac{1}{1-qx^k}\right) = \sum_{k=1}^{\infty} \pi_q(k) \sum_{\nu=1}^{\infty} \frac{x^{k\nu}}{k\nu} \cdot k \\ &= \sum_{n=1}^{\infty} \frac{x^n}{n} \cdot \left(\sum_{d|n} d \cdot \pi_q(d) \right) \end{aligned}$$

und damit $q^n = \sum_{d|n} d \cdot \pi_q(d)$ für alle $n \in \mathbb{N}$. Mit der Möbiusschen Umkehrformel (Satz 1.5.5) folgt

$$n \cdot \pi_q(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d$$

wegen $1 + q + \ldots + q^{n-1} = \frac{q^n-1}{q-1}$ und somit $\pi_q(n) > 0$. □

Definition 1.5.6. Es sei K ein Körper und $f, g \in K[x]$. Unter der Restklasse $g \bmod (f)$ versteht man $g \bmod (f) := \{g + h \cdot f \colon h \in K[x]\}$. Unter dem Restklassenring $K[x]/(f)$ versteht man die Menge der Restklassen mit der Addition und der Multiplikation, die folgendermaßen definiert sind:

$$\begin{aligned} g \bmod (f) + h \bmod (f) &= (g+h) \bmod (f) \\ g \bmod (f) \cdot h \bmod (f) &= (g \cdot h) \bmod (f). \end{aligned}$$

Man sieht leicht, dass das Ergebnis der Verknüpfungen von der Auswahl der Repräsentanten unabhängig ist.

Satz 1.5.12. *Es sei K ein endlicher Körper mit $|K| = q$, und $f_0 \in K[x]$ sei ein irreduzibles Polynom mit $\deg f_0 = n \in \mathbb{N}$. Dann ist der Restklassenring $R = K[x]/(f_0)$ ein Körper mit q^n Elementen.*

Beweis. Jedes $r \in R$ ist eindeutig darstellbar in der Form $r(x) = a_0 + a_1 x + \ldots + a_{n-1}x^{n-1} + (f_0)$. Da es für jedes der a_ν für $0 \leq \nu \leq n-1$ genau q Möglichkeiten gibt, folgt $|R| = q^n$.
Alle Körperaxiome sind klar mit Ausnahme der Existenz des multiplikativen Inversen.
Es sei nun $g \bmod (f_0) \in R\backslash\{0\}$. Nach Satz 1.5.8 (Euklidischer Algorithmus) gibt es $s, t \in K[x]$ mit $sg + tf_0 = 1$. Dann ist aber $(s \bmod (f_0)) \cdot (g \bmod (f_0)) = 1 \bmod (f_0)$. □

Satz 1.5.13. *Es sei $q = p^m$ eine Primzahlpotenz. Dann gibt es einen Körper $\mathbb{F}_q$ mit q Elementen.*

Beweis. Dies folgt aus den Sätzen 1.5.6, 1.5.11 und 1.5.12. □

Satz 1.5.14. *Es sei $q = p^m$ eine Primzahlpotenz. Dann gibt es $q-1$ paarweise OLQ und eine projektive Ebene der Ordnung q.*

Beweis. Dies folgt aus den Sätzen 1.3.1, 1.4.2 und 1.5.13. □

Kapitel 2

Verallgemeinerte Designs, weitere Konstruktionsmethoden für Orthogonale Lateinische Quadrate

2.1 Der Satz von Mc Neish

Im letzten Kapitel haben wir gesehen, dass wir für $n = p^m$ die maximale Anzahl $N(n) = n - 1$ von paarweisen OLQ erhalten können. Der Satz von Mc Neish ermöglicht nun zwar nicht die Maximalzahl, aber immer noch viele OLQ zu erhalten, die paarweise orthogonal sind, wenn in der Primfaktorzerlegung von n nur große Primzahlpotenzen vorkommen.

Satz 2.1.1. *Es sei $n = l \cdot m$ mit $l, m \in \mathbb{N}$. Dann gilt $N(n) \geq \min\{N(l), N(m)\}$.*

Beweis. Es seien $k = \min\{N(l), N(m)\}$ sowie $A^{(1)} = (a_{ij}^{(1)}), \ldots, A^{(k)} = (a_{ij}^{(k)})$ mit $1 \leq i, j \leq l$ paarweise verschiedene OLQ der Ordnung l und $B^{(1)} = (b_{ij}^{(1)}), \ldots, B^{(k)} = (b_{ij}^{(k)})$ mit $1 \leq i, j \leq m$ paarweise verschiedene OLQ der Ordnung m. Für $1 \leq h \leq k$ wird die Matrix $C^{(h)}$ als die folgende $(l \cdot m \times l \cdot m)$-Matrix

$$C^{(h)} := \begin{pmatrix} (a_{11}^{(h)}, B^{(h)}) & (a_{12}^{(h)}, B^{(h)}) & \ldots & (a_{1l}^{(h)}, B^{(h)}) \\ \vdots & & \ddots & \\ (a_{l1}^{(h)}, B^{(h)}) & (a_{l2}^{(h)}, B^{(h)}) & \ldots & (a_{ll}^{(h)}, B^{(h)}) \end{pmatrix}$$

mit $h = 1, \ldots, k$ definiert, wobei die Teilmatrizen über

$$(a_{ij}^{(h)}, B^{(h)}) := \begin{pmatrix} (a_{ij}^{(h)}, b_{1,1}^{(h)}) & (a_{ij}^{(h)}, b_{1,2}^{(h)}) & \ldots & (a_{ij}^{(h)}, b_{1,m}^{(h)}) \\ (a_{ij}^{(h)}, b_{2,1}^{(h)}) & (a_{ij}^{(h)}, b_{2,2}^{(h)}) & \ldots & (a_{ij}^{(h)}, b_{2,m}^{(h)}) \\ \vdots & & \ddots & \\ (a_{ij}^{(h)}, b_{m,1}^{(h)}) & \ldots & \ldots & (a_{ij}^{(h)}, b_{m,m}^{(h)}) \end{pmatrix}$$

gegeben sind. Man überprüft leicht, dass die $C^{(h)}$ paarweise orthogonal sind. □

Satz 2.1.2. *(Mc Neish)*
Es sei $n = p_1^{\gamma_1} \cdots p_r^{\gamma_r}$ die kanonische Primfaktorzerlegung von n. Dann ist

$$N(n) \geq \min_{1 \leq i \leq r} \{p_i^{\gamma_i} - 1\}.$$

Beweis. Wiederholte Anwendung von Satz 1.5.12 ergibt $N(n) \geq \min_{1 \leq i \leq r} N(p_i^{\gamma_i})$.
Die Behauptung folgt dann aus Satz 1.5.13. □

2.2 Orthogonale Lateinische Quadrate und Orthogonale Schemata

Probleme über OLQ werden oft übersichtlicher, wenn man sie in der Sprache der orthogonalen Schemata formuliert.

Definition 2.2.1. Es sei $n \in \mathbb{N}$ und $\mathcal{M}$ eine Menge von n Symbolen.
Zwei Zeilenvektoren $\vec{v}_1 = (x_1, \ldots, x_{n^2})$ bzw. $\vec{v}_2 = (y_1, \ldots, y_{n^2})$ der Länge n^2 mit $x_i, y_i \in \mathcal{M}$ heißen orthogonal, wenn unter den geordneten Paaren (x_i, y_i) für $1 \leq i \leq n^2$ jedes Paar $(u, v) \in \mathcal{M}^2$ genau einmal vorkommt.

Definition 2.2.2. Es sei $n \in \mathbb{N}$ und $\mathcal{M}$ eine Menge von n Symbolen.
Ein orthogonales Schema $OS(n, s)$ der Ordnung n und Tiefe s ist eine Matrix mit s Zeilen und n^2 Spalten, deren Einträge Symbole aus $\mathcal{M}$ sind, so dass jedes Paar von Zeilen orthogonal ist.

Folgende Tatsache ist unmittelbar klar:

Satz 2.2.1. *Ist eine $s \times n^2$- Matrix ein $OS(n, s)$, so bleibt diese Eigenschaft auch nach einer beliebigen Permutation der Zeilen oder Spalten oder einer Umbenennung der Elemente einer einzelnen Zeile erhalten.*

Satz 2.2.2. *Es seien $k, n \in \mathbb{N}$ mit $n \geq 2$. Es existiert genau dann ein $OS(n, k+2)$, wenn es eine Menge von k paarweise verschiedene OLQ der Ordnung n gibt.*

Beweis. Wir führen nur eine Richtung des Beweises.
Es sei ein $OS(n, k+2)$ gegeben. OBdA nehmen wir an, dass die Menge der Symbole $\mathcal{M} = \{1, \ldots, n\}$ ist. Durch Permutation der Spalten können wir dann ein $OS(n, k+2)$ erhalten, dessen erste zwei Zeilen $\vec{v}_1$ und $\vec{v}_2$ die Form

$$\begin{pmatrix} 1 & 1 & \ldots & 1 & 2 & 2 & \ldots & 2 & \ldots & n & n & \ldots & n \\ 1 & 2 & \ldots & n & 1 & 2 & \ldots & n & \ldots & 1 & 2 & \ldots & n \end{pmatrix}$$

haben. Es seien $\vec{v}_3, \ldots, \vec{v}_{k+2}$ die übrigen Zeilenvektoren. Wir konstruieren die Lateinischen Quadrate $A^{(j)} = (a_{li}^{(j)})$ mit $1 \leq j \leq k$ und $1 \leq l, i \leq n$ wie folgt:
Für $1 \leq l, i \leq n$ sei $s(l, i)$ die eindeutig bestimmte Spalte, deren erste beiden Komponenten den Spaltenvektor $(l, i)^T$ bilden. □

2.3 Verallgemeinerte Designs

In Kapitel I hatten wir Designs mit fester Blockgröße betrachtet. In der Folge lassen wir auch unterschiedliche Größe von Blöcken zu.

Definition 2.3.1. Ein (pairwise balanced design) $BIB(v, k_1, \ldots, k_m, \lambda)$ ist ein Paar $(\mathcal{D}, \mathcal{B})$, wobei $\mathcal{D}$ eine Menge von v Objekten und $\mathcal{B}$ eine Menge von Teilmengen von $\mathcal{D}$ ist, die Blöcke genannt werden. Die Größe der Blöcke sind durch die Zahlen k_i mit $k_i < v$ gegeben und jedes Paar von Objekten tritt in genau λ Blöcken auf.
Die Menge der Blöcke mit k_i Elementen heißen die i- te equiblock component.
Ein clearset ist eine Vereinigung von equiblock components, in denen zwei verschiedene Blöcke disjunkt sind. Wir schreiben $BIB(v, k_1, \ldots k_r; k_{r+1}, \ldots, k_m)$, falls $\lambda = 1$ und die ersten r equiblock components einen clearset bilden.

Satz 2.3.1. *Falls es ein* $BIB(v, k_1, \dots k_r; k_{r+1}, \dots, k_m)$ *gibt, gilt*

$$N(v) \geq \min\{N(k_1), \dots, N(k_r); N(k_{r+1}) - 1, \dots, N(k_m) - 1\}.$$

Beweis. Es sei

$$c = \min\{N(k_1) + 2, \dots, N(k_r) + 2; N(k_{r+1}) + 1, \dots, N(k_m) + 1\}.$$

Nach Satz 2.2.2 gibt es orthogonale Schemata $A_i = OS(k_i, c)$ für $i = 1, \dots, r$ und orthogonale Schemata $D_i = OS(k_i, c+1)$ für $i = r+1, \dots, m$. Die Matrix D_i ist eine Matrix vom Typ $(c+1) \times k_i^2$ mit den Elementen $1, \dots, k_i$.
Wir verschieben nun die k_i Spalten mit einer "1" in der ersten Zeile an den Anfang und nummerieren die Elemente in den restlichen Zeilen so um, dass die ersten k_i Spalten von D_i die folgende Form haben:

$$\begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & 2 & \dots & k_i \\ \vdots & \vdots & & \vdots \\ 1 & 2 & \dots & k_i \end{pmatrix}$$

Aus D_i mit $i = r+1, \dots, m$ bilden wir Matrizen A_i, indem wir die erste Zeile und die ersten k_i Spalten von D_i streichen.
Die A_i sind folglich Matrizen vom Typ $c \times (k_i^2 - k_i)$, welche in jedem Paar von verschiedenen Zeilen alle Spalten $(u, w)^T$ mit $u \neq w$ und $u, w = 1, \dots, k_i$, aber keine Spalten $(u, u)^T$ hat.
Es seien $S_1, S_2, \dots, S_b$ die Blöcke des BIB. Die Elemente $1, \dots, k_i$ von A_i ersetzen wir durch Umbenennung durch die Elemente der Blöcke $S_1, S_2, \dots, S_b$ und erhalten die Matrizen B_i.
Es sei E eine Matrix, deren Spaltenzahl die Anzahl der Objekte des BIB ist, die nicht in dem clearset vorkommen, in der jede Spalte eines dieser Elemente c- mal enthält. Durch Aneinanderreihen bilden wir die Matrix $C = (B_1, B_2, \dots, B_b, E)$.
Wir behaupten nun, dass C ein $OS(v, c)$ ist.
Dazu betrachten wir zwei Zeilen $\vec{v}_h$ und $\vec{v}_k$. Es seien $u \neq w$ zwei verschiedene Objekte des BIB. Dann gibt es genau einen Block S_j, der sowohl u als auch w enthält, und in den zugehörigen B_j wird eine Spalte $(u, w)^T$ in den zwei Zeilen $\vec{v}_h, \vec{v}_k$ sein. Es kommen u und w in keiner Spalte der B_i mit $i \neq j$ und in keiner Spalte von E vor.
Es sei u ein Objekt des clearset, und es sei $u \in S_j$. Dann gibt es in den Zeilen $\vec{v}_h$ und $\vec{v}_k$ von B_j eine Spalte $(u, u)^T$. Ist u nicht im clearset, so gibt es in E in den Zeilen $\vec{v}_h$ und $\vec{v}_k$ eine Spalte $(u, u)^T$.
Folglich sind $\vec{v}_h$ und $\vec{v}_k$ zueinander orthogonal und C ist ein $OS(v, c)$.
Infolgedessen gibt es nach Satz 2.2.2 nun $c - 2$ OLQ, und der Satz ist bewiesen.

Illustration:
clearset: Blöcke der equiblock- components zu k_i mit $1 \leq i \leq r$:

$$A_i = \begin{pmatrix} \\ \quad OS \quad \\ \\ \end{pmatrix}$$

mit c Zeilen.
Blöcke der equiblock- components zu k_i mit $r+1 \leq i \leq m$:

$$D_i = \left(\begin{array}{ccccccc|cccc} 1 & 1 & & \dots & & 1 & & x & x & \dots & x \\ 1 & 2 & \dots & u & \dots & k_i & & & & & \\ \vdots & & & \vdots & & & & & & & \\ 1 & 2 & \dots & u & \dots & k_i & & & & & \end{array}\right)$$

mit $c+1$ Zeilen und

$$A_i = \begin{pmatrix} x & x & \dots x & x \\ & & & \end{pmatrix}$$

Über $A_i \to B_i$ werden die Elemente $\{1, \dots, k_i\}$ in Elemente des Blocks S_i umbenannt. Dann ist

$$C = \left(\begin{array}{c|c||c|c} B_1 & B_2 & B_b & E \\ \begin{pmatrix} u \\ u \end{pmatrix} & & \begin{pmatrix} u \\ w \end{pmatrix} \quad \begin{pmatrix} \not{u} \\ \not{u} \end{pmatrix} & \begin{pmatrix} u \\ u \end{pmatrix} \end{array} \right)$$

Der erste Vektor ist dabei in genau einem Block wegen der clearset- Eigenschaft.
Die Vektoren $(u, w)^T$ sind für Paare $u \neq w$ in S_j enthalten.
Der gestrichene Vektor wurde beim Übergang von D_i zu A_i entfernt.
Schließlich ist der letzte Vektor für u nicht aus dem clearset. □

Definition 2.3.2. Ein BIB heißt auflösbar mit r Replikationen, wenn die Menge $\mathcal{B}$ der Blöcke so in r Teilmengen, Replikationen genannt, aufgeteilt werden können, dass für jede Replikation $\mathcal{R}$ jedes Objekt des BIB in genau einem Block von $\mathcal{R}$ enthalten ist.

Beispiel 2.3.1. Es sei K ein Körper mit $|K| = q$. Die affine Ebene $(K^2, \mathcal{G})$, wobei $\mathcal{G}$ die Menge der Geraden von K^2 ist, ist ein Design $D(q^2, q^2+q, q+1, q, 1)$ mit der Blockmenge $\mathcal{G}$. Dabei ist $(K^2, \mathcal{G})$ auflösbar mit $q+1$ Replikationen, wobei die Replikationen aus den Geraden einer Parallelenschar bestehen. Jedes Objekt, d.h. jeder Punkt, ist in genau einem Block, also einer Geraden, einer Replikation, d.h. einer Parallelenschar enthalten.

Wir betrachten nun noch weitere Verallgemeinerte Designs, die group divisible designs:
Während bisher der Parameter λ, der angibt, in wievielen Blöcken ein Paar von Objekten gemeinsam vorkommt, konstant war, treten nun für verschiedene Paare verschiedene Werte von λ- insgesamt zwei verschiedene- auf. Der Wert 0 kann auch auftreten.

Definition 2.3.3. Ein group divisible design $G\mathcal{D}(\nu; k, m; \lambda_1, \lambda_2)$ ist ein Tripel $(\mathcal{D}, \mathcal{B}, \mathcal{G})$, wobei $\mathcal{D}$ eine Menge von ν Objekten, $\mathcal{B}$ eine Menge von Teilmengen von $\mathcal{D}$, Blöcke genannt, und $\mathcal{G}$ eine Partition von $\mathcal{D}$ in Teilmengen von je m Objekten, Gruppen genannt, ist, so dass folgendes gilt:

1. Jeder Block enthält k Objekte.
2. Zwei Objekte derselben Gruppe treten zusammen in λ_1 Blöcken auf, während zwei Objekte von verschiedenen Gruppen zusammen in λ_2 Blöcken auftreten.

Wir werden hier nur den Fall $\lambda_1 = 0$ und $\lambda_2 = 1$ verwenden.

Definition 2.3.4. Ein auflösbares $G\mathcal{D}(\nu; k, m; \lambda_1, \lambda_2)$ mit r Replikationen ist ein $G\mathcal{D}(\nu; k, m; \lambda_1, \lambda_2)$, wenn die Menge $\mathcal{B}$ der Blöcke so in r Teilmengen, Replikationen genannt, aufgeteilt werden können, dass für jede Replikation $\mathcal{R}$ jedes Objekt des $G\mathcal{D}$ in genau einem Block von $\mathcal{R}$ enthalten ist.

Satz 2.3.2. *Wenn $k \leq N(m)+1$ gilt, dann existiert ein auflösbares $G\mathcal{D}(km; k, m; 0, 1)$ mit m Replikationen.*

Beweis. Wegen $k \leq N(m)+1$ existiert ein $OS(m, k+1)$. OBdA können wir annehmen, dass die Menge der Symbole $\{1, 2, \dots, m\}$ und dass die letzte Zeile von der Form

$$1, \dots, 1, 2, \dots, 2, \dots, m, \dots, m$$

ist.

Als Abschnitt A_r mit $1 \leq r \leq m$ bezeichnen wir nun die Teilmatrix aus den Spalten mit unterstem Element r. Daraus erhalten wir eine Matrix $\mathcal{M}$ vom Typ (k, m^2) mit r Teilmatrizen $\mathcal{M}_r$ mit $1 \leq r \leq m$ wie folgt:
Wir streichen jetzt die letzte Zeile und ersetzen die Zahl i in der j- ten Zeile durch das Paar (i, j). Nun geht $\mathcal{M}_r$ aus den Spalten des Abschnitts A_r hervor, und wir können das gewünschte Design $G\mathcal{D}(km; k, m; 0, 1)$ konstruieren.
Die Objekte des $G\mathcal{D}$ sind die Paare (i, j) der Matrix $\mathcal{M}$. Ihre Anzahl ist km. Die Blöcke des Designs sind die Spalten von $\mathcal{M}$. Die r- te Replikation ist die Menge der Spalten der Teilmatrix $\mathcal{M}_r$.
Die j_0- te Gruppe ist die Menge der Paare (i, j) mit der zweiten Koordinate $j = j_0$. Objekte mit derselben zweiten Koordinate, d.h. aus derselben Gruppe, treten nie gemeinsam im selben Block auf. Wegen der Orthogonalität der j- ten und j'- ten Zeile des OS treten Objekte mit verschiedenen zweiten Koordinaten i und j' zusammen in genau einem Block auf.
Jedes Objekt (i, j) tritt in der r- ten Replikation, d.h. in der Teilmatrix $\mathcal{M}_r$ wegen der Orthogonalität der j- ten und der untersten Zeile des OS genau einmal auf.
Damit hat das Design die gewünschten Eigenschaften. □

Satz 2.3.3. *Es existiere ein auflösbares $G\mathcal{D}(\nu; k, m; 0, 1)$ mit m Replikationen. Weiter sei $1 \leq x < m$. Dann gilt $N(\nu + x) \geq \min\{N(m), N(x), N(k) - 1, N(k + 1) - 1\}$.*

Beweis. Wir konstruieren nun aus den Objekten, Blöcken und Gruppen des Designs $G\mathcal{D}(\nu; k, m; 0, 1)$ ein $BIB(\nu + x; x, m; k, k + 1)$ wie folgt:
Wir machen aus den Blöcken der Größe k der i- ten Replikation mit $1 \leq i \leq x$ einen Block des BIB der Größe $k + 1$, indem wir ein neues Objekt Y_i hinzufügen.
Die Blöcke der restlichen Replikationen lassen wir unverändert und definieren sie ebenfalls als Blöcke des BIB der Größe k. Die Gruppen $\mathcal{G}_i$ des $G\mathcal{D}$ machen wir zu Blöcken des BIB der Größe m. Schließlich machen wir die neuen Objekte $Y_1, \ldots, Y_x$ zu einem Block $Y = \{Y_1, \ldots, Y_x\}$ des BIB.
Wir haben zu zeigen, dass wir auf diese Weise ein $BIB(\nu + x; x, m; k, k + 1)$ erhalten.
Es ist klar, dass die Anzahl der Objekte $\nu + x$ und die Größe der Blöcke x, m, k bzw. $k + 1$ ist. Es ist auch klar, dass die equiblock- component- Blöcke der Größe m, die aus der Gruppe $\mathcal{G}$ bestehen, und die equiblock- component der Größe x einen clearset bilden.
Es bleibt zu zeigen, dass jedes Paar (u, w) an Objekten in genau einem Block auftritt.
Fall 1:
Es sind u und w Objekte des $G\mathcal{D}$ und gehören nicht zur selben Gruppe. Nach Definition des $G\mathcal{D}$ gibt es genau einen Block B des $G\mathcal{D}$ mit $u, w \in B$.
Fall 2:
Es sind u und w Objekte des $G\mathcal{D}$ und gehören zur selben Gruppe. Dann gibt es genau einen Block, nämlich Y, zu dem u und w gehören. Das Paar (u, w) tritt in keinem der Blöcke des BIB und auch nicht in $\{Y_1, \ldots, Y_x\}$ auf.
Fall 3:
Es gilt $u \in G\mathcal{D}$ und $w = Y_i$ mit $1 \leq i \leq x$. Es gibt dann genau einen Block B_u der i- ten Replikation mit $u \in B_u$. Dann ist das Paar (u, w) in dem Block $B_u \cup \{Y_i\}$ enthalten und in keinem anderen.
Fall 4:
Es sei $u = Y_i$ und $w = Y_j$ mit $i \neq j$. Dann ist (u, w) im Block Y_x enthalten.
Damit ist alles bewiesen. □

Satz 2.3.4. *Es sei $k \leq N(m) + 1$ mit $1 \leq x < m$. Dann gilt*

$$N(km + x) \geq \min\{N(m), N(x), N(k) - 1, N(k + 1) - 1\}.$$

Beweis. Nach Satz 2.3.2 existiert ein $G\mathcal{D}(km; k, m; 0, 1)$. Die Behauptung folgt dann aus Satz 2.3.3, wenn wir $\nu = km$ setzen. □

Bemerkung 2.3.1. Satz 2.3.4 erlaubt es, untere Schranken für $N(m)$ zu erhalten, indem man n in der Form $n = km + x$ schreibt, wobei die in der Primfaktorisierung von k, $k + 1$, m und x vorkommenden Primzahlpotenzen sämtlich groß sind. Dies ist ein rein zahlentheoretisches Problem, das mit Siebmethoden, die wir im nächsten Abschnitt besprechen wollen, behandelt werden kann.

Beispiel 2.3.2. Es sei $n = 1300 = 2^2 \cdot 5^2 \cdot 13$. Der Satz von Mc Neish ergibt $N(n) \geq 2^2 - 1 = 3$. Nun ist $n = 31 \cdot 41 + 29$. Satz 2.3.4 ergibt

$$N(n) \geq \min\{N(41), N(29), N(31) - 1, N(32) - 1) = 28.$$

Kapitel 3

Siebmethoden

3.1 Grundlagen aus der elementaren Primzahltheorie

Definition 3.1.1. Die Primzahlzählfunktion $\pi(x)$ ist durch

$$\pi(x) := |\{p \in \mathbb{P} \colon p \leq x\}| = \sum_{p \leq x} 1$$

definiert. Der Summationsindex p bedeutet hier und im folgenden, dass über Primzahlen summiert wird.

Schon Euklid wusste, dass $\pi(x) \to \infty$ für $x \to \infty$ gilt. Gauß vermutete um 1792 die Gültigkeit des sogenannten Primzahlsatzes:

$$\pi(x) \sim \frac{x}{\log x} \ (x \to \infty) \quad \text{d.h.} \quad \lim_{x \to \infty} \frac{\pi(x)}{x/\log x} = 1.$$

Dies konnte jedoch erst 1896 von Hadamard und de la Vallée- Poussin gezeigt werden.
Wir werden den Beweis in dieser Vorlesung nicht geben. Uns genügen schwächere Ergebnisse, die mit denen von Tschebyschew zusammenhängen, der 1850 zuerst die wahre Größenordnung von $\pi(x)$ bestimmte.

Satz 3.1.1. *Es gibt Konstanten $c_1 > 0$ und $c_2 > 0$, so dass für alle $x \geq x_0$*

$$c_1 \cdot \frac{x}{\log x} \leq \pi(x) \leq c_2 \cdot \frac{x}{\log x}$$

gilt.

Beweis. Übungen. □

Ergebnisse der Analytischen Zahlentheorie haben die Form

"Unbekannte Funktion = Hauptglied + Restglied"

oder "Unbekannte Funktion $\leq$ Explizite Funktion".
Zur Vereinfachung der Formulierung hat Edmund Landau die nach ihm benannte O- und o- Symbole eingeführt.

Definition 3.1.2. Es seien $f(x)$ und $g(x)$ zwei Funktionen, die für genügend große positive x definiert sind, und es sei $f(x)$ beliebig komplex, $g(x) > 0$ eventuell nur für genügend große x. Dann soll

$$f(x) = O(g(x)) \quad \text{bzw.} \quad f(x) = o(g(x)) \ (x \to \infty)$$

bedeuten, dass für genügend große x folgendes gilt:

$$|f(x)| \leq A \cdot g(x) \quad \text{für passendes } A > 0 \quad \text{bzw.} \quad \frac{|f(x)|}{|g(x)|} \underset{x\to\infty}{\to} 0.$$

Analog mögen die Beziehungen

$$f(x) = O(g(x)) \quad \text{bzw.} \quad f(x) = o(g(x)) \quad (x \to a^+) \quad \text{oder} \quad (x \to a^-)$$

definiert sein, wobei $g(x) > 0$ für x nahe bei a vorausgesetzt ist.

Satz 3.1.2. *Der Primzahlsatz kann in der Form*

$$\pi(x) = \frac{x}{\log x} + o\left(\frac{x}{\log x}\right) \quad (x \to \infty) \quad \textit{oder auch} \quad \pi(x) = \frac{x}{\log x} \cdot (1 + o(1)) \quad (x \to \infty)$$

geschrieben werden.

Satz 3.1.3. *(Mertens)*
Es gilt

$$\sum_{p \leq x} \frac{\log p}{p} = \log x + O(1) \quad (x \to \infty).$$

Beweis. Es sei $N = [x]$, und wir untersuchen die Primfaktorzerlegung von $N!$. Es sei $N! = \prod_{p \leq N} p^{\gamma(p)}$. Zur Bestimmung des Exponenten $\gamma(p)$ beachten wir, dass von den Zahlen $1, \ldots, N$ genau $\left[\frac{x}{p}\right]$ durch p teilbar sind, $\left[\frac{x}{p^2}\right]$ durch p^2 usw. Damit gilt

$$\gamma(p) = \left[\frac{x}{p}\right] + \left[\frac{x}{p^2}\right] + \ldots + \left[\frac{x}{p^{r(p)}}\right] = \frac{x}{p} + O(1) + O\left(\frac{x}{p^2}\right)$$

mit $r(p) = \frac{\log x}{\log p}$. Somit folgt wegen $\pi(x) = O\left(\frac{x}{\log x}\right)$

$$\log N! = x \cdot \sum_{p \leq x} \frac{\log p}{p} + O(x).$$

Mittels der Stirlingschen Formel $\log N! = N \cdot \log N - N + O(\log N)$ folgt

$$x \cdot \sum_{p \leq x} \frac{\log p}{p} = x \log x + O(x)$$

und damit

$$\sum_{p \leq x} \frac{\log p}{p} = \log x + O(1).$$

□

Von Interesse ist auch die Summe $\sum_{p \leq x} \frac{1}{p}$. Diese erhält man, indem man aus der Summe $\sum_{p \leq x} \frac{\log p}{p}$ die "Gewichte" $\log p$ entfernt. Eine Methode zur Entfernung oder Hinzufügung regulärer Gewichte liefert die Abelsche Partielle Summation.

Satz 3.1.4. *(Abelsche Partielle Summation)*
Es seien $a < b$ reelle Zahlen und $c_1, , c_2, \ldots$ komplexe Zahlen. Weiter sei $c(x) = \sum_{a<n\leq x} c_n$. Dann gilt

i) diskrete Version:
Es seien $f_1, \ldots, f_n$ komplexe Zahlen mit $(\Delta f)_n = f_{n+1} - f_n$. Dann gilt

$$\sum_{a<n\leq b} c_n f_n = c(b) f_{[b]} - \sum_{a<n\leq b-1} c(n)(\Delta f)_n.$$

ii) kontinuierliche Version:
Es sei f auf $[a, b]$ stetig differenzierbar. Dann ist

$$\sum_{a<n\leq b} c_n f(n) = c(b)f(b) - \int_a^b c(t)f'(t)\,dt.$$

Beweis. i) Es ist

$$\begin{aligned}\sum_{a<n\leq b} c_n f_n &= \sum_{a<n\leq b} (c(n) - c(n-1)) \cdot f_n = \sum_{a<n\leq b} c(n) f_n - \sum_{a<n\leq b-1} c(n) f_{n+1} \\ &= c(b) f_{[b]} - \sum_{a<n\leq b-1} c(n)(f_{n+1} - f_n).\end{aligned}$$

Dies beweist (i).

ii) Es seien die Voraussetzungen von Teil ii) erfüllt. Zudem setzen wir $f_n := f(n)$. Für $t \in [n, n+1)$ ist $c(t) = c(n)$, und es gilt

$$f_{n+1} - f_n = \int_n^{n+1} f'(t)\,dt,$$

also

$$c(n) \cdot (f_{n+1} - f_n) = \int_n^{n+1} c(t)f'(t)\,dt. \tag{1}$$

Außerdem ist

$$c(b)f(b) - c([b])f_{[b]} = \int_{[b]}^b c(t)f'(t)\,dt. \tag{2}$$

Damit folgt aus i), (1) und (2)

$$\sum_{a<n\leq b} c_n f_n = c(b)f(b) - (c(b)f(b) - c([b])f([b])) - \int_a^{[b]} c(t)f'(t)\,dt = c(b)f(b) - \int_a^b c(t)f'(t)\,dt.$$

□

Satz 3.1.5. *Es gibt eine Konstante $b \in \mathbb{R}$ mit*

$$\sum_{p\leq x} \frac{1}{p} = \log\log x + b + O\left(\frac{1}{\log x}\right).$$

Beweis. Wir wenden Satz 3.1.4 ii) mit

$$c_n = \begin{cases} \frac{\log p}{p}, & \text{falls } n = p \in \mathbb{P} \\ 0 & \text{sonst} \end{cases}$$

und $f(t) = \frac{1}{\log t}$ sowie $a = \frac{3}{2}$ an. Wir erhalten

$$\begin{aligned} \sum_{p \le x} \frac{1}{p} &= \sum_{p \le x} \frac{\log p}{p} \cdot \frac{1}{\log p} \\ &= \left(\sum_{p \le x} \frac{\log p}{p} \right) \cdot \frac{1}{\log x} + \int_{3/2}^{x} \left(\sum_{p \le t} \frac{\log p}{p} \right) \frac{dt}{t \log^2 t}. \end{aligned}$$

Nach Satz 3.1.3 ist $\sum_{p \le t} \frac{\log p}{p} = \log t + r(t)$ mit $r(t) = O(1)$. Also gilt

$$\begin{aligned} \sum_{p \le x} \frac{1}{p} &= (\log x + r(x)) \cdot \frac{1}{\log x} + \int_{3/2}^{x} \frac{dt}{t \log t} + \int_{3/2}^{x} \frac{r(t)}{t \log^2 t}\, dt \\ &= 1 + \frac{r(x)}{\log x} + \log\log x - \log\log \frac{3}{2} + \int_{3/2}^{\infty} \frac{r(t)}{t \log^2 t}\, dt + O\left(\frac{1}{\log x}\right) \\ &= \log\log x + b + O\left(\frac{1}{\log x}\right) \end{aligned}$$

mit

$$b = 1 - \log\log \frac{3}{2} + \int_{3/2}^{\infty} \frac{r(t)}{t \log^2 t}\, dt.$$

□

3.2 Formulierung des allgemeinen Siebproblems

In den Bezeichnungen folgen wir hier weitgehend dem Buch von Halberstam und Richert. Auch die Ergebnisse sind diesem Buch entnommen.

Siebmethoden werden verwendet, um die Anzahl der Glieder einer endlichen Folge $\mathcal{A}$ von ganzen Zahlen abzuschätzen, die durch keine Primzahl p aus der Primzahlmenge $\mathcal{P}$ teilbar sind, die unter einer Schranke $z > 1$ liegen.

Definition 3.2.1. Es sei $\mathcal{A}$ eine endliche Folge ganzer Zahlen, die gegebene Werte mehrfach annehmen kann. Es sei $\mathcal{P}$ eine Menge von Primzahlen und $z \ge 2$ mit $z \in \mathbb{R}$. Die Menge aller Primzahlen sei $\mathbb{P}$. Dann definieren wir

$$S(\mathcal{A}; \mathcal{P}, z) = |\{a \in \mathcal{A} \colon p | a,\ p \in \mathcal{P} \Rightarrow p > z\}|$$

und $P(z) = \prod_{p<z} p$. In den Anwendungen wird die Folge $\mathcal{A}$ gewöhnlich von einem Parameter abhängen, der gegen unendlich strebt.
Man kann Ergebnisse über $S(\mathcal{A}; \mathcal{P}, z)$ unter Angaben sehr allgemeiner Art über die Folge $\mathcal{A}$ erhalten. Wir werden die Art dieser Informationen in der Folge beschreiben.
Für eine quadratfreie Zahl d sei $\mathcal{A}_d = \{a \in \mathcal{A} \colon a \equiv 0 \bmod d\}$ die Teilfolge der durch d teilbaren Zahlen.
Über $\mathcal{A}$ benötigen wir Informationen der folgenden Art:
Für $X > 1$ und eine multiplikative Funktion ω_0 setzen wir

$$r_d := |\mathcal{A}_d| - \frac{\omega_0(d)}{d} X$$

für $\mu(d) \neq 0$.

Von dem Restglied r_d wird gewünscht, dass es (wenigstens im Mittel) klein ist. Dann liefert X eine gute Approximation für die Mächtigkeit von $\mathcal{A}$, während Approximationen für $\mathcal{A}_d$ durch $\frac{\omega_0(d)}{d}X$ gegeben sind.

Beispiel 3.2.1. Es sei $\mathcal{A} = \{n\colon x - y < n \leq x\}$ mit $1 < y \leq x$. Dann liefert $S(\mathcal{A}, \mathbb{P}, z)$ obere Schranken für die Anzahl der Primzahlen im Intervall $[x-y, y]$. Falls $z \geq x^{1/2}$ ist, ergeben sich auch untere Schranken. Setzen wir $X = y$, $\omega_0(p) = 1$ für alle $p \in \mathbb{P}$ und $\omega_0(d) = 1$ für quadratfreie d, so erhalten wir $|r_d| \leq 1$.

Beispiel 3.2.2. Es sei $\mathcal{A} = \{n^2+1\colon n \leq x\}$. Die Teilbarkeit von n^2+1 durch ein quadratfreies d hängt nur von den Restklassen von n mod d ab. Es sei $d = 2^\epsilon p_1 \cdots p_r$ die Zerlegung von d in Primfaktoren mit $\epsilon \in \{0,1\}$ und $2 < p_1 < p_2 < \ldots < p_r$. Nach dem Chinesischen Restsatz ist die Kongruenz

$$n^2 + 1 \equiv 0 \bmod d \tag{1}$$

zum System der Kongruenzen

$$\begin{cases} n^2 + 1 \equiv 0 \bmod 2^\epsilon \\ n^2 + 1 \equiv 0 \bmod p_1 \\ \vdots \\ n^2 + 1 \equiv 0 \bmod p_r \end{cases} \tag{2}$$

äquivalent.
Für eine ungerade Primzahl p hat $n^2+1 \equiv 0 \bmod p$ zwei Lösungen modulo p, falls $\left(\frac{-1}{p}\right) = 1$ gilt, also im Falle $p \equiv 1 \bmod 4$. Andernfalls besitzt $n^2+1 \equiv 0 \bmod p$ keine Lösung modulo p, falls $\left(\frac{-1}{p}\right) = -1$ gilt, also für $p \equiv 3 \bmod 4$. Für $p = 2$ hat $n^2+1 \equiv 0 \bmod p$ die eine Lösung $n \equiv 1 \bmod 2$.
Die Anzahl $l(d)$ der Lösungen von (1) ist somit durch

$$l(d) = \begin{cases} 0, & \text{falls } p|d \text{ für eine Primzahl } p \equiv 3 \bmod 4 \\ 2^r & \text{sonst,} \end{cases}$$

gegeben. Letzteres bedeutet damit $d = 2^\epsilon p_1 \cdots p_r$, $\epsilon \in \{0,1\}$ und $p_i \equiv 1 \bmod 4$ für $1 \leq i \leq r$.
Nun lässt sich das Intervall $[0, x]$ in $\left[\frac{x}{d}\right]$ Teilintervalle $I_k = [(k-1)d, kd)$ mit $1 \leq k \leq \left[\frac{x}{d}\right]$ der Länge d und im Falle $\frac{x}{d} \notin \mathbb{N}$ ein Teilintervall $I_{k+1} = [\left[\frac{x}{d}\right], x)$ der Länge kleiner d einteilen. Jedes I_k mit $1 \leq k \leq \left[\frac{x}{d}\right]$ enthält $l(d)$ Elemente von $\mathcal{A}_d$, während I_{k+1} weniger als d enthält. Somit folgt

$$|\mathcal{A}_d| = \left[\frac{x}{d}\right] \cdot l(d) + \theta_d \tag{3}$$

mit $0 \leq \theta_d < d$. Als geeigente Wahl für den Parameter X und die multiplikative Funktion ω_0 ergibt sich somit $X = x$ und $\omega_0 = l(d)$. Aus (3) ergibt sich somit für $r_d = |\mathcal{A}_d| - \frac{\omega_0}{d} \cdot X$ schließlich $|r_d| < d$.

Beispiel 3.2.3. Es sei $\mathcal{A} = \{n \cdot (n+2)\colon n \leq x\}$. Für $z = x^{1/2}$ ist $S(\mathcal{A}, \mathbb{P}, z) = \pi_2(x) + O(\sqrt{x})$, wobei $\pi_2(x) = |\{p \leq x-2\colon p+2 \in \mathbb{P}\}|$ die Anzahl der Primzahlzwillinge kleiner gleich x bedeute. Für $z \leq x^{1/2}$ ergeben sich obere Schranken für $\pi_2(x)$.
Es sei $d = 2^\epsilon p_1 \cdots p_r$ die Zerlegung von d in Primfaktoren mit $\epsilon \in \{0,1\}$ und $2 < p_1 < p_2 < \ldots < p_r$. Wiederum ist nach dem Chinesischen Restsatz die Kongruenz

$$n^2 + 2n \equiv 0 \bmod d \tag{1}$$

zum System der Kongruenzen

$$\begin{cases} n^2 + 2n \equiv 0 \bmod 2^\epsilon \\ n^2 + 2n \equiv 0 \bmod p_1 \\ \vdots \\ n^2 + 2n \equiv 0 \bmod p_r \end{cases} \tag{2}$$

äquivalent.

Nun hat $n \cdot (n+2) \equiv 0 \bmod p$ die eine Lösung $n \equiv 0 \bmod 2$ für $p = 2$ und sonst die zwei Lösungen $n \equiv 0 \bmod p$ und $n \equiv -2 \bmod p$. Die Anzahl $l(d)$ der Lösungen von (1) ist somit 2^r. Wie im vorigen Beispiel 3.2.2 teilen wir das Intervall $[0, x]$ in $\left[\frac{x}{d}\right]$ Teilintervalle $I_k = [(k-1)d, kd)$ mit $1 \leq k \leq \left[\frac{x}{d}\right]$ der Länge d und möglicherweise ein zusätzliches Intervall der Länge kleiner d ein.
Jedes I_k mit $1 \leq k \leq \left[\frac{x}{d}\right]$ enthält $l(d)$ Elemente von $\mathcal{A}_d$, während I_{k+1} höchstens $l(d)$ enthält. Somit folgt

$$|\mathcal{A}_d| = \left[\frac{x}{d}\right] \cdot l(d) + \theta_d \tag{3}$$

mit $0 \leq \theta_d < l(d)$. Als geeigente Wahl für den Parameter X und die multiplikative Funktion ω_0 ergibt sich somit $X = x$ und $\omega_0 = l(d) = 2^r$, wobei r die Anzahl der ungeraden Primfaktoren von d darstellt.

3.3 Einschluss- Ausschluss- Prinzip, Einschluss- Ausschluss- Ungleichungen

Das Sieb des Erathosthenes, das einfachste Sieb, das wir im nächsten Abschnitt behandeln werden, ist eine zahlentheretische Version des Einschluss- Ausschluss- Prinzips. Danach werden wir das Reine Brunsche Sieb behandeln, ein leistungsfähigeres Sieb, das auf der Einschluss- Ausschluss- Ungleichung beruht.

Satz 3.3.1. *Es seien $k, \nu \in \mathbb{N}$. Dann gilt*

$$\sigma(\nu, k) := \sum_{m=0}^{k-1} (-1)^m \binom{\nu}{m} = (-1)^{k-1} \binom{\nu - 1}{k - 1}.$$

Beweis. Wir führen den Beweis durch Induktion nach k durch.
Induktionsanfang: $k = 1$:
Die Behauptung folgt wegen

$$\sigma(\nu, 1) = \sum_{m=0}^{0} (-1)^m \binom{\nu}{m} = \binom{\nu}{0} = (-1)^{1-1} \binom{\nu - 1}{0}.$$

Induktionsschritt: $k \to k + 1$:
Es gelte die Induktionyhypothese für ein $k \in \mathbb{N}$. Zudem gilt

$$\binom{\nu}{k} - \binom{\nu - 1}{k - 1} = \binom{\nu - 1}{k}$$

und damit

$$\sigma(\nu, k+1) = (-1)^k \binom{\nu}{k} + \sigma(\nu, k) \underset{(IH)}{=} (-1)^k \cdot \left(\binom{\nu}{k} - \binom{\nu - 1}{k - 1} \right) = (-1)^k \binom{\nu - 1}{k}.$$

□

Für den Rest von Abschnitt 3.3 treffen wir folgende Annahmen:
Es sei $\mathcal{M}$ eine endliche Menge von Objekten, $\mathcal{M}_1, \ldots, \mathcal{M}_r$ seien Teilmengen von $\mathcal{M}$. Es sei $\mathcal{S}$ die Menge der Objekte von $\mathcal{M}$, die keiner der Teilmengen $\mathcal{M}_i$ angehören.

Satz 3.3.2. *(Einschluss- Ausschluss- Prinzip)*
Es gilt

$$|\mathcal{S}| = |\mathcal{M}| + \sum_{k=1}^{r} (-1)^k \cdot \sum_{(j_1, \ldots, j_k)} |\mathcal{M}_{j_1} \cap \ldots \cap \mathcal{M}_{j_k}|.$$

Bevor wir Satz 3.3.2 beweisen, fragen wir uns, was wir erhalten, wenn wir die Summe auf der rechten Seite nicht über sämtliche k, sondern nur über $1 \leq k \leq t$ mit $t \in \mathbb{N}$ und $t \leq r$ erstrecken.

Definition 3.3.1. Es sei $t \in \mathbb{N}_0$ mit $t \leq r$. Unter der Einschluss- Ausschluss- Summe $E(t)$ verstehen wir

$$E(t) := |\mathcal{M}| + \sum_{k=1}^{t} (-1)^k \cdot \sum_{(j_1,\ldots,j_k)} |\mathcal{M}_{j_1} \cap \ldots \cap \mathcal{M}_{j_k}|.$$

Wir werden nun sehen, dass wir für ungerade Werte von t eine untere Schranke und für gerade Werte von t eine obere Schranke für $|\mathcal{S}|$ erhalten.

Satz 3.3.3. *(Einschluss- Ausschluss- Ungleichungen)*
Es sei $s \in \mathbb{N}_0$. Dann haben wir

$$E(2s+1) \leq |\mathcal{S}| \leq E(2s).$$

Beweis. (Beweis der Sätze 3.3.2 und 3.3.3)
Es sei $\mathcal{M} = \{r_1, \ldots, r_l\}$. Für $1 \leq i \leq l$ sei $n(r_i)$ die Anzahl der Mengen $\mathcal{M}_j$ mit $r_i \in \mathcal{M}_j$. Wir erhalten durch die Änderung der Summationsreihenfolge

$$\begin{aligned} E(t) &= |\mathcal{M}| + \sum_{k=1}^{t} (-1)^k \cdot \sum_{(j_1,\ldots,j_k)} |\mathcal{M}_{j_1} \cap \ldots \cap \mathcal{M}_{j_k}| \\ &= \sum_{i=1}^{l} \left(1 + \sum_{1 \leq k \leq \min\{n(r_i),t\}} (-1)^k \cdot \sum_{\substack{(j_1,\ldots,j_k) \\ r_i \in \mathcal{M}_{j_1} \cap \ldots \cap \mathcal{M}_{j_k}}} 1 \right). \end{aligned}$$

Es gibt $\binom{n(r_i)}{k}$ Möglichkeiten, aus den $n(r_i)$ Mengen, die r_i enthalten, die k Mengen $\mathcal{M}_{j_1}, \ldots, \mathcal{M}_{j_k}$ auszuwählen. Deshalb erhalten wir für die innere Summe

$$\sum_{\substack{(j_1,\ldots,j_k) \\ r_i \in \mathcal{M}_{j_1} \cap \ldots \cap \mathcal{M}_{j_k}}} 1 = \binom{n(r_i)}{k}$$

und somit

$$E(t) = \sum_{i=1}^{l} \left(1 + \sum_{1 \leq k \leq \min\{n(r_i),t\}} (-1)^k \cdot \binom{n(r_i)}{k} \right).$$

Es sei $n(r_i) \geq 1$. Nach Satz 3.3.1 ist

$$(-1)^t \cdot \left(1 + \sum_{1 \leq k \leq \min\{n(r_i),t\}} (-1)^k \cdot \binom{n(r_i)}{k} \right) = (-1)^{2t} \cdot \binom{n(r_i)-1}{t}.$$

Dies verschwindet aber für $t \geq n(r_i)$ und ist ansonsten nichtnegativ. Dies beendet den Beweis. □

3.4 Das Sieb des Erathosthenes

Satz 3.4.1. *(Sieb des Erathosthenes)*
Mit den Definitionen und Bezeichnungen von Abschnitt 3.2 haben wir

$$S(\mathcal{A},\mathcal{P},z)=\sum_{d|P(z)}\mu(d)|\mathcal{A}_d|.$$

Beweis. • Beweis nach dem Einschluss- Ausschluss- Prinzip:
Es ist $S(\mathcal{A},\mathcal{P},z)=|\{m\in\mathcal{A}\colon m\notin\mathcal{A}_p,\ \forall p\in\mathcal{P},\ p<z\}|$, wobei $p_1<p_2<\ldots<p_r$ die Primzahlen von $\mathcal{P}$ kleiner z seien. Damit ist nach Satz 3.3.2 (Einschluss- Ausschluss- Prinzip)

$$S(\mathcal{A},\mathcal{P},z)=|\mathcal{A}|+\sum_{k=1}^{r}(-1)^k\cdot\sum_{(j_1,\ldots,j_k)}|\mathcal{A}_{p_{j_1}}\cap\ldots\cap\mathcal{A}_{p_{j_k}}|. \tag{1}$$

Wir setzen $d=p_{j_1}\cdots p_{j_k}$. Dann ist $\mathcal{A}_{p_{j_1}}\cap\ldots\cap\mathcal{A}_{p_{j_k}}=\mathcal{A}_d$ und $(-1)^k=\mu(d)$. Aus (1) erhalten wir

$$S(\mathcal{A},\mathcal{P},z)=\sum_{d|P(z)}\mu(d)|\mathcal{A}_d|.$$

• Zahlentheoretischer Beweis:
Es gilt

$$S(\mathcal{A},\mathcal{P},z)=\sum_{a\in\mathcal{A}\colon\,(a,P(z))=1}1=\sum_{a\in\mathcal{A}}\sum_{\substack{d|a\\ d|P(z)}}\mu(d)=\sum_{d|P(z)}\mu(d)\sum_{\substack{a\in\mathcal{A}\\ a\equiv 0 \bmod d}}1=\sum_{d|P(z)}\mu(d)|\mathcal{A}_d|.$$

□

Beispiel 3.4.1. Es sei $\mathcal{A}=\{1,\ldots,100\}$. Wir wenden Satz 3.4.1 mit $z=6$ und $\mathcal{P}=\mathbb{P}$ an und erhalten so eine obere Schranke für $\pi(100)$. Es ist

$$\begin{aligned}S(\mathcal{A},\mathbb{P},z) &= \sum_{d|P(z)}\mu(d)|\mathcal{A}_d\\ &= |\mathcal{A}|-|\mathcal{A}_2|-|\mathcal{A}_3|-|\mathcal{A}_5|+|\mathcal{A}_6|+|\mathcal{A}_{10}|+|\mathcal{A}_{15}|-|\mathcal{A}_{30}|\\ &= 100-50-33-20+16+10+6-3=26.\end{aligned}$$

Damit gilt $\pi(100)\le S(\mathcal{A},\mathbb{P},z)+\pi(6)-1=28$.

Mit etwas mehr Rechnung können wir auch den genauen Wert von $\pi(100)$ bestimmen. Hierzu beachten wir, dass jede zusammengesetzte Zahl n einen Teiler kleiner gleich $n^{1/2}$ besitzt.
Es ist damit $\pi(100)=S(\mathcal{A},\mathbb{P},z)+\pi(10)-1$, und wir erhalten

$$\begin{aligned}S(\mathcal{A},\mathbb{P},10) &= \sum_{d|P(z)}\mu(d)|\mathcal{A}_d\\ &= |\mathcal{A}|-|\mathcal{A}_2|-|\mathcal{A}_3|-|\mathcal{A}_5|-|\mathcal{A}_7|+|\mathcal{A}_6|+|\mathcal{A}_{10}|+|\mathcal{A}_{14}|+|\mathcal{A}_{15}|+|\mathcal{A}_{21}|+|\mathcal{A}_{35}|\\ &\quad -|\mathcal{A}_{30}|-|\mathcal{A}_{42}|-|\mathcal{A}_{70}|-|\mathcal{A}_{105}|+|\mathcal{A}_{210}|\\ &= 100-50-33-20-14+16+10+6+4+2-3-2-1=22.\end{aligned}$$

Damit folgt $\pi(100)=S(\mathcal{A},\mathbb{P},10)+\pi(10)-1=25$

In Anwendungen sind wir an Situationen interessiert, in denen $\mathcal{A}$ von einem Parameter x abhängt. Für $x \to \infty$ wird auch $\mathcal{A} \to \infty$ gelten. Wir benötigen Informationen der Art, wie sie in Abschnitt 3.2 beschrieben wurden. Wir orientieren uns auch den den in Abschnitt 3.2 eingeführten Bezeichnungen. Zudem treffen wir noch folgende Definitionen:

Definition 3.4.1. Die arithmetische Funktion ω sei durch

$$\omega(p) = \begin{cases} \omega_0(p) & \text{für } p \in \mathcal{P} \\ 0 & \text{für } p \notin \mathcal{P} \end{cases}$$

sowie $\omega(1) = 1$ und $\omega(d) = \prod_{p|d} \omega(p)$ für $\mu(d) \neq 0$ definiert. Weiter sei

$$R_d := |\mathcal{A}_d| - \frac{\omega(d)}{d} \cdot X$$

für $\mu(d) \neq 0$ sowie

$$\begin{aligned} W(z) &:= \prod_{p<z} \left(1 - \frac{\omega(p)}{p}\right) \\ V(z) &:= \prod_{p<z} \left(1 - \frac{1}{p}\right). \end{aligned}$$

Bemerkung 3.4.1. Gehören sämtliche Primfaktoren von d zu $\mathcal{P}$ und ist $\mu(d) \neq 0$, so haben wir $\omega(d) = \omega_0(d)$ und $R_d = r_d$.

Satz 3.4.2. *Für $z \geq 2$ gilt*

$$S(\mathcal{A}, \mathcal{P}, z) = XW(z) + \theta \cdot \sum_{d|P(z)} |R_d|$$

mit $|\theta| \leq 1$.

Beweis. Nach Satz 3.4.1 haben wir

$$S(\mathcal{A}, \mathcal{P}, z) = \sum_{d|P(z)} \mu(d)|\mathcal{A}_d|.$$

Wir verwenden nun die Approximation

$$|\mathcal{A}_d| = \frac{\omega(d)}{d} \cdot X + R_d$$

mit dem "Hauptglied" $\frac{\omega(d)}{d} \cdot X$ und dem "Restglied" R_d und trennen die Beiträge der Hauptglieder und der Restglieder. Wir erhalten

$$S(\mathcal{A}, \mathcal{P}, z) = X \cdot \sum_{d|P(z)} \mu(d) \cdot \frac{\omega(d)}{d} + \sum_{d|P(z)} \mu(d) \cdot R_d.$$

Es sei $f(d) = \mu(d)\frac{\omega(d)}{d}$. Dies ist eine multiplikative Funktion. Damit ist auch die Faltung $f \star 1$ mit

$$(f \star 1)(n) = \sum_{d|n} \mu(d) \cdot \frac{\omega(d)}{d}$$

multiplikativ.

Also gilt

$$\sum_{d|P(z)} \mu(d) \cdot \frac{\omega(d)}{d} = \prod_{p|P(z)} \sum_{d|p} \mu(d) \cdot \frac{\omega(d)}{d} = \prod_{p<z} \left(1 - \frac{\omega(p)}{p}\right) = W(z).$$

Wegen $|\mu(d)| = 1$ ist

$$\left| \sum_{d|P(z)} \mu(d) R_d \right| \leq \sum_{d|P(z)} |R_d|,$$

also

$$S(\mathcal{A}, \mathcal{P}, z) = XW(z) + \theta \cdot \sum_{d|P(z)} |R_d|.$$

□

Satz 3.4.3. *Es gibt eine Konstante $C_0 > 0$, so dass*

$$V(z) = \frac{C_0}{\log z} \cdot \left(1 + O\left(\frac{1}{\log z}\right)\right)$$

für $z \to \infty$ gilt.

Beweis. Wir haben

$$V(z) = \prod_{p<z} \left(1 - \frac{1}{p}\right) = \sum_{p<z} \left(-\frac{1}{p} + \left(\log\left(1 - \frac{1}{p}\right) + \frac{1}{p}\right)\right). \tag{1}$$

Aus der Taylorreihe

$$\log(1-x) = -x + \sum_{k=2}^{\infty} \frac{(-1)^k}{k} \cdot x^k$$

für $|x| < 1$ folgt

$$\left|\log\left(1 - \frac{1}{p}\right) + \frac{1}{p}\right| \leq \frac{1}{p^2}. \tag{2}$$

Damit ist nach dem Majorantenkriterium die unendliche Reihe

$$\sum_{p} \log\left(1 - \frac{1}{p}\right) + \frac{1}{p}$$

konvergent, und wir haben nach (2)

$$\sum_{p<z} \left(-\frac{1}{p} + \left(\log\left(1 - \frac{1}{p}\right) + \frac{1}{p}\right)\right) = c_1 + O\left(\frac{1}{z}\right).$$

Aus (1) erhalten wir

$$\log V(z) = -\sum_{p<z} \frac{1}{p} + c_1 + O\left(\frac{1}{z}\right)$$

und nach Satz 3.1.4

$$\log V(z) - \log\log z - b + c_1 + O\left(\frac{1}{\log z}\right).$$

Die Behauptung folgt durch Exponentation, wenn wir $C_0 = e^{c_1 - b}$ setzen. □

Bemerkung 3.4.2. Es kann gezeigt werden, dass $C_0 = e^{-\gamma}$ mit der Euler- Mascheronischen- Konstante

$$\gamma = \lim_{N\to\infty}\left(\sum_{k=1}^{N}\frac{1}{k} - \log N\right)$$

gilt.

Beispiel 3.4.2. Es sei $\mathcal{A} = \{n\colon x - y < n \leq x\}$, wobei $1 < y \leq x$. Für $z \geq 2$ wollen wir eine Aussage über $S(\mathcal{A}, \mathcal{P}, z)$ erhalten. Nach Beispiel 3.4.1 empfiehlt sich die Wahl $X = y$ und $\omega_0(p) = 1$ für alle p. Wir erhalten für $r_d = |\mathcal{A}_d| - \frac{\omega_0(d)}{d}X$ dann $|r_d| \leq 1$. Nach Definition 3.4.1 ist wegen $\mathcal{P} = \mathbb{P}$ dann $\omega_0(p) = \omega(p)$ und $R_d = r_d$. Es ist

$$W(z) = V(z) = \prod_{p<z}\left(1 - \frac{1}{p}\right).$$

Damit erhalten wir nach den Sätzen 3.4.2 und 3.4.3 mit $\theta|, |\theta'| \leq 1$

$$S(\mathcal{A}, \mathcal{P}, z) = XW(z) + \theta \cdot \sum_{d|P(z)} |R_d| = \frac{C_0 y}{\log z} \cdot \left(1 + O\left(\frac{1}{\log z}\right)\right) + \theta' \cdot 2^{\pi(z)}.$$

Wir erhalten nur dann ein nichttriviales Ergebnis, wenn $2^{\pi(z)} \leq y$ gilt. Ist $y = x$, so ist dies für $z_0 = c \log x \log\log x$ erfüllt, und wir erhalten

$$\pi(x) \leq S(\mathcal{A}, \mathcal{P}, z) = O\left(\frac{x}{\log\log x}\right),$$

ein Ergebnis, das wesentlich schwächer als Tschebyschews Ergebnis $\pi(x) = O\left(\frac{x}{\log x}\right)$ ist. Andererseits erhalten wir für $y \geq x^{\epsilon}$ mit einem festen $\epsilon > 0$ für die Anzahl der Primzahlen im Intervall $(x - y, x)$ die Größe $\pi(x) - \pi(x - y) = O\left(\frac{y}{\log\log x}\right)$.

3.5 Das Reine Brunsche Sieb

Definition 3.5.1. Für $d \in \mathbb{N}$ bedeute $\nu(d)$ die Anzahl der verschiedenen Primfaktoren von d, also

$$\nu(d) := \sum_{p|d} 1.$$

Satz 3.5.1. *(Reines Brunsches Sieb, allgemeine Version)*
Es sei $s \in \mathbb{N}_0$. Mit den Bezeichnungen von Abschnitt 3.2 haben wir

$$\sum_{\substack{d|P(z)\\ \nu(d)\leq 2s+1}} \mu(d)|\mathcal{A}_d| \leq S(\mathcal{A}, \mathcal{P}, z) \leq \sum_{\substack{d|P(z)\\ \nu(d)\leq 2s}} \mu(d)|\mathcal{A}_d|.$$

Beweis. Es ist

$$S(\mathcal{A}, \mathcal{P}, z) = \left|\{m \in \mathcal{A}\colon m \notin \mathcal{A}_p \forall p \in \mathcal{P},\ p < z\}\right|.$$

Es seien $p_1 < p_2 < \ldots < p_r$ die Primzahlen von $\mathcal{P}$ kleiner z. Dann ist nach Satz 3.3.3 (Einschluss-Ausschluss- Ungleichungen)

$$|\mathcal{A}| + \sum_{k=1}^{2s+1}(-1)^k \cdot \sum_{(p_{j_1},\ldots,p_{j_k})} |\mathcal{A}_{p_{j_1}} \cap \ldots \cap \mathcal{A}_{p_{j_k}}| \leq S(\mathcal{A}, \mathcal{P}, z) \leq |\mathcal{A}| + \sum_{k=1}^{2s}(-1)^k \cdot \sum_{(p_{j_1},\ldots,p_{j_k})} |\mathcal{A}_{p_{j_1}} \cap \ldots \cap \mathcal{A}_{p_{j_k}}|. \tag{1}$$

Wir setzen $d = p_{j_1} \cdots p_{j_k}$, woraus $\mathcal{A}_{p_{j_1}} \cap \ldots \cap \mathcal{A}_{p_{j_k}} = \mathcal{A}_d$ und $(-1)^k = \mu(d)$ folgt. Dann folgt die Behauptung direkt aus (1). □

Um eine schärfere Aussage zu erhalten, nehmen wir noch an, dass für die Menge $\mathcal{A}_d$ Approximationen der in Abschnitt 3.2 beschriebenen Art gegeben sind. Für die multiplikative Funktion ω setzen wir zusätzlich voraus, dass folgende Bedingungen erfüllt sind:

$$\omega(p) \leq A_0 \tag{Ω_0}$$

und

$$0 \leq \frac{\omega(p)}{p} \leq 1 - \frac{1}{A_1} \tag{Ω_1}$$

mit positiven Konstanten A_0 und A_1.

Zur Vorbereitung des Beweises des Hauptresultats treffen wir zunächst eine Definition und beweisen ein Lemma:

Definition 3.5.2. Es sei $r \in \mathbb{N}$ und $d|P(z)$. Wir setzen

$$\chi^{(r)}(d) = \begin{cases} 1, & \text{falls } \nu(d) \leq r \\ 0 & \text{sonst} \end{cases}$$

und $\sigma^{(r)}(n) = \sum_{d|n} \mu(d)\chi^{(r)}(d)$ sowie

$$g(d) = \frac{\omega(d)}{d \cdot \prod_{p|d}\left(1 - \frac{\omega(p)}{p}\right)}.$$

Weiter sei B_0 eine Konstante mit

$$\sum_{p<z} \frac{1}{p} \leq \log\log z + B_0$$

für alle $z \geq 2$. Nach Satz 3.1.4 gibt es eine solche Konstante.

Lemma 3.5.1. *Es sei $d|P(z)$ und $\nu(n) = v$. Dann haben wir*

$$\sum_{d|n} \mu(d)\chi^{(r)}(d) = (-1)^r \binom{v-1}{r}.$$

Insbesondere haben wir für $\nu(n) < r$ dann $\sigma^{(r)}(n) = 0$.

Beweis. Die Anzahl der Teiler von n mit $\nu(d) = m$ ist $\binom{v}{m}$. Für solche Teiler ist dann $\mu(d) = (-1)^m$. Damit gilt

$$\sum_{d|n} \mu(d)\chi^{(r)}(d) = \sum_{m=0}^{\infty} (-1)^m \binom{v}{m} = (-1)^r \binom{v}{r}$$

nach Satz 3.3.1. □

Satz 3.5.2. *(Ω_0), (Ω_1))*
Es sei $z \geq 2$ und λ so gewählt, dass $0 < \lambda e^{1+\lambda} \leq 1$ und $r_0 = \left[\frac{A_0 A_1}{\lambda} \cdot (\log\log z + B_0)\right] + 1$. Dann gibt es Konstanten θ und θ' mit $|\theta| \leq 1$ und $|\theta'| \leq 1$, so dass

$$S(\mathcal{A}, \mathcal{P}, z) = XW(z) \cdot \left(1 + \theta\left(\lambda e^{1+\lambda}\right)^{(A_0 A_1/\lambda)\cdot(\log\log z + B_0)}\right) + \theta' \cdot \sum_{\substack{d|P(z) \\ \nu(d) \leq r_0+1}} |R_d|$$

gilt.

Beweis. Es sei $s \in \mathbb{N}_0$ und $r \in \{2s, 2s+1\}$.
Wir spalten die untere Schranke $r = 2s+1$ und die obere Schranke $r = 2s$ von Satz 3.5.1 in Hauptglied und Restglied auf, indem wir die Approximation

$$|\mathcal{A}_d| = \frac{\omega(d)}{d} X + R_d$$

benützen. Wir erhalten

$$\sum_{\substack{d|P(z) \\ \nu(d)\leq r}} \mu(d)|\mathcal{A}_d| = X \cdot \sum\nolimits_H^{(r)} + \sum\nolimits_R^{(r)} \tag{1}$$

mit

$$\sum\nolimits_H^{(r)} = \sum_{d|P(z)} \mu(d)\chi^{(r)}(d)\frac{\omega(d)}{d} \tag{2}$$

bzw.

$$\sum\nolimits_R^{(r)} = \sum_{d|P(z)} \mu(d)\chi^{(r)}(d)R_d. \tag{3}$$

Wir formen zunächst $\sum_H^{(r)}$ um.
Es wird dabei angestrebt, einen Vergleich zwischen dem Term $X \cdot \sum_H^{(r)}$ in (1) und dem Term $XW(z)$ zu erhalten, der sich beim Sieb des Erathosthenes als Hauptglied ergibt.
Zunächst ergibt die Möbiussche Umkehrformel

$$\chi^{(r)}(d) = \sum_{\delta|d} \mu(d/\delta)\sigma^{(r)}(\delta).$$

Einsetzen von (2) ergibt

$$\begin{aligned}
\sum\nolimits_H &= \sum_{d|P(z)} \mu(d)\chi^{(r)}(d)\frac{\omega(d)}{d} = \sum_{d|P(z)} \frac{\omega(d)}{d} \sum_{\delta|d} \mu\left(\frac{d}{\delta}\right)\sigma^{(r)}(\delta) \\
&\underset{d=\delta\cdot t}{=} \sum_{\delta|P(z)} \sigma^{(r)}(\delta)\frac{\omega(\delta)}{\delta} \sum_{t|P(z)/\delta} \mu(t)\frac{\omega(t)}{t} = \sum_{\delta|P(z)} \sigma_r(\delta)\frac{\omega(\delta)}{\delta} \prod_{p|P(z)/\delta} \left(1 - \frac{\omega(p)}{p}\right) \\
&= W(z) \cdot \sum_{\delta|P(z)} \frac{\omega(\delta)}{\delta \cdot \prod_{p|\delta}\left(1 - \frac{\omega(p)}{p}\right)} \cdot \sigma_r(\delta) = W(z) \cdot \left(1 + \sum_{1<\delta|P(z)} \sigma^{(r)}(\delta)g(\delta)\right),
\end{aligned}$$

also

$$\sum\nolimits_H = W(z) \cdot \left(1 + \sum_{1<\delta|P(z)} \sigma^{(r)}(\delta)g(\delta)\right). \tag{4}$$

Als nächstes wollen wir nun eine Schranke für den "Fehler im Hauptglied" erhalte. Mit Lemma 3.5.1 folgt

$$\begin{aligned}
\left|\sum_{1<d|P(z)} \sigma^{(r)}(d)g(d)\right| &\leq \sum_{1<d|P(z)} \binom{\nu(d)}{r} g(d) = \sum_{m=r}^{\nu(P(z))} \binom{m}{r} \sum_{\substack{1<d|P(z)) \\ \nu(d)=m}} g(d) \\
&\leq \sum_{m=r}^{\infty} \binom{m}{r} \cdot \frac{1}{m!} \cdot \left(\sum_{p<z} g(p)\right)^m = \frac{1}{r!} \cdot \left(\sum_{p<z} g(p)\right)^r \cdot \exp\left(\sum_{p<z} g(p)\right),
\end{aligned}$$

folglich

$$\left|\sum_{1<d|P(z)} \sigma^{(r)}(d)g(d)\right| \leq \frac{1}{r!}\cdot\left(\sum_{p<z} g(p)\right)^r \cdot \exp\left(\sum_{p<z} g(p)\right). \tag{5}$$

Es sei nun λ mit $0a < \lambda \cdot e^{1+\lambda} < 1$ gegeben. Damit ist nach der Definition von r_0

$$\sum_{p<z} g(p) \leq \lambda \cdot r_0. \tag{6}$$

Indem wir die Schranke $\frac{1}{r!} \leq \left(\frac{e}{r}\right)^r$ für $r \in \mathbb{N}$ benützen, die durch Umformen aus $\left(1+\frac{1}{r}\right)^r < e$ entsteht, erhalten wir mit $r = r_0$

$$\frac{1}{r_0!}\cdot\left(\sum_{p<z} g(p)\right)^{r_0} \cdot \exp\left(\sum_{p<z} g(p)\right) \leq \left(\frac{e}{r_0}\right)^{r_0} \cdot (\lambda \cdot r_0)^{r_0} \cdot e^{\lambda r_0} = \left(\lambda \cdot e^{1+\lambda}\right)^{r_0}. \tag{7}$$

Es gilt auch

$$\sum_{p<z} g(p) \leq \lambda \cdot (r_0+1).$$

Durchführung der obigen Rechnungen für $r = r_0 + 1$ ergibt

$$\frac{1}{(r_0+1)!}\cdot\left(\sum_{p<z} g(p)\right)^{r_0+1} \cdot \exp\left(\sum_{p<z} g(p)\right) \leq \left(\lambda \cdot e^{1+\lambda}\right)^{r_0+1}. \tag{8}$$

Wir wenden nun Satz 3.5.1 an und erhalten mit (1)

$$X \cdot \sum\nolimits_H^{(r_1)} + \sum\nolimits_R^{(r_1)} \leq S(\mathcal{A}, \mathcal{P}, z) \leq X \cdot \sum\nolimits_H^{(r_2)} + \sum\nolimits_R^{(r_2)}$$

mit $\{r_1, r_2\} = \{r_0, r_0+1\}$ und mit (7) und mit (8)

$$XW(z)\cdot\left(1-\left(\lambda\cdot e^{1+\lambda}\right)^{r_0}\right) - \sum_{\substack{d|P(z)\\ \nu(d)\leq\nu_0+1}} |R_d| \leq S(\mathcal{A},\mathcal{P},z) \leq XW(z)\cdot\left(1+\left(\lambda\cdot e^{1+\lambda}\right)^{r_0}\right) + \sum_{\substack{d|P(z)\\ \nu(d)\leq\nu_0+1}} |R_d|.$$

Daraus folgt die Behauptung. □

Beispiel 3.5.1. Es sei $\mathcal{A} = \{n\colon n \leq x\}$ und $\mathcal{P} = \mathbb{P}$.
Nach Beispiel 3.2.1 sind geeignete Approximationen durch $X = x$ und $\omega(d) = 1$ gegeben.
Die Bedingungen (Ω_0): $\omega(p) \leq A_0$ und (Ω_1): $0 \leq \frac{\omega(p)}{p} \leq 1 - \frac{1}{A_1}$ sind mit $A_0 = 1$ und $A_1 = 2$ erfüllt.
Wir wählen $\lambda = \frac{1}{5}$ und $z = \exp\left(\frac{1}{20}\frac{\log x}{\log\log x}\right)$ und erhalten $r_0 = [10(\log\log z + B_0)] + 1$. Es sei $d|P(z)$ und $\nu(d) \leq r_0 + 1$. Dann gilt

$$d \leq z^{r_0+1} \leq \exp\left(\frac{1}{20}\frac{\log x}{\log\log x}\cdot(10\log\log x + B_0) + 2\right) = O(x^{3/5})$$

und damit

$$\sum_{\substack{d|P(z)\\ \nu(d)\leq r_0+1}} |R_d| = O(x^{3/5}).$$

Weiter ist

$$W(z) = \frac{C_0}{\log z}\cdot\left(1+O\left(\frac{1}{\log z}\right)\right) = O\left(\frac{\log x}{\log\log x}\right).$$

Damit folgt aus Satz 3.5.1

$$\pi(x) = O\left(x \cdot \frac{\log\log x}{\log x}\right).$$

Dies ist wesentlich schärfer als das aus dem Sieb des Erathosthenes erhaltene Ergebnis

$$\pi(x) = O\left(\frac{x}{\log\log x}\right).$$

mit $z = c\frac{\log x}{\log\log x}$, aber immer noch schwächer als das Tschebyschewsche Resultat

$$\pi(x) = O\left(\frac{x}{\log x}\right).$$

Beispiel 3.5.2. Es sei $\mathcal{A} = \{n \cdot (n+2) \colon n \leq x\}$ und $\mathcal{P} = \mathbb{P}$. Nach Beispiel 3.2.3 ist eine geeignete Wahl für die Parameter X und die multiplikative Funktion ω durch $X = x$ und

$$\omega(p) = \begin{cases} 1 & \text{für } p = 2 \\ 2 & \text{für } p > 2 \end{cases}$$

gegeben. Es gilt dann $|R_d| < d$.
Die Bedingungen (Ω_0): $\omega(p) \leq A_0$ und (Ω_1): $0 \leq \frac{\omega(p)}{p} \leq 1 - \frac{1}{A_1}$ sind mit $A_0 = 2$ und $A_1 = 3$ erfüllt. Wir wählen $\lambda = \frac{1}{5}$ und $z = \exp\left(\frac{1}{120}\frac{\log x}{\log\log x}\right)$ und erhalten $r_0 = [30(\log\log z + B_0)] + 1$. Es sei $d|P(z)$ und $\nu(d) \leq r_0 + 1$. Dann gilt

$$d \leq z^{r_0+1} \leq \exp\left(\frac{1}{120}\frac{\log x}{\log\log x} \cdot (30\log\log x + B_0) + 2\right) = O(x^{1/3})$$

und damit

$$\sum_{\substack{d|P(z) \\ \nu(d) \leq r_0+1}} |R_d| = O(x^{2/3}).$$

Es ist

$$W(z) = \prod_{p<z}\left(1 - \frac{\omega(p)}{p}\right) = \prod_{2<p<z}\left(1 - \frac{2}{p}\right) = O\left(\exp\left(\sum_{2<p<z}\log\left(1 - \frac{2}{p}\right)\right)\right) = O\left(\frac{1}{\log^2 z}\right)$$

für $z \to \infty$. Damit ergibt sich für $\pi_2(x)$, die Anzahl der Primzahlzwillinge kleiner gleich x

$$\pi_2(x) = O\left(x \cdot \frac{(\log\log x)^2}{\log^2 x}\right).$$

Dieses war historisch der erste Erfolg der Brunschen Methode.

Als Folgerung haben wir

Satz 3.5.3. *Es gilt*

$$\sum_{p \colon p+2 \in \mathbb{P}} \frac{1}{p} < \infty.$$

Beweis. Partielle Summation ergibt

$$\sum_{\substack{p:\ p+2\in\mathbb{P}\\ p+2\le x}} \frac{1}{p} \le \frac{\pi_2(x)}{x} + \int_2^x \frac{\pi_2(t)}{t}\,dt.$$

Nun ist

$$\lim_{x\to\infty} \frac{\pi_2(x)}{x} = 0$$

und

$$\int_2^x \frac{\pi_2(t)}{t}\,dt = O\left(\int_2^x \frac{(\log\log t)^2}{t\cdot\log^2 t}\,dt\right) < \infty.$$

□

3.6 Kombinatorische Siebe

Das Sieb des Erathosthenes und das Reine Brunsche Sieb sind Beispiele Kombinatorischer Siebe.
Als Vorbereitung zur Behandlung des Brunschen Siebes, das auch in diese Kategorie fällt, wollen wir hier ein paar allgemeine Prinzipien der Kombinatorischen Siebe behandeln.
Allen Kombinatorischen Sieben gemeinsam ist die Anwendung von Ungleichungen

$$\sum_{d|P(z)} \mu(d)\chi_2(d)|\mathcal{A}_d| \le S(\mathcal{A},\mathcal{P},z) \le \sum_{d|P(z)} \mu(d)\chi_1(d)|\mathcal{A}_d| \tag{1}$$

mit $\chi_\nu \in \{0,1\}$.
Die Ungleichungen (1) beruhen auf Ungleichungen für die Funktionen σ_ν, die durch

$$\sigma_\nu(n) = \sum_{d|n} \mu(d)\chi_\nu(d) \tag{2}$$

mit $\sigma_\nu(1) = \chi_\nu(1) = 1$ für $\nu = 1, 2$ definiert sind.
Im einfachsten Fall, dem Sieb des Erathosthenes, wird $\chi_1(d) = \chi_2(d) = 1$ für alle $d|P(z)$ gewählt, und wir erhalten

$$\sigma_1(d) = \sigma_2(d) = \sigma_0(d) := \sum_{d|n} \mu(d) = \begin{cases} 1 & \text{für } n = 1 \\ 0 & \text{sonst.} \end{cases}$$

Im allgemeinen Kombinatorischen Sieb sind die Ungleichungen für σ_1 und σ_2 durch

$$\sigma_2(d) \le \sigma_0(d) \le \sigma_1(d) \tag{3}$$

für alle $d|P(z)$, d.h. $\sigma_2(d) \le 0 \le \sigma_1(d)$ für $d > 1$ und $\sigma_2(1) = \sigma_1(1) = 1$ gegeben.

Aus den Ungleichungen (3) folgen dann die Ungleichungen (1) durch Änderung der Summationsreihenfolge:

$$\begin{aligned}\sum_{d|P(z)} \mu(d)\chi_\nu(d)|\mathcal{A}_d| &= \sum_{a\in\mathcal{A}}\sum_{d|a} \mu(d)\chi_\nu(d) \\ &= \sum_{\substack{a\in\mathcal{A}\\ d|P(z)}} \sigma_\nu((a,P(z))) \begin{cases} \geq S(\mathcal{A},\mathcal{P},z) & \text{für } \nu=1 \\ \leq S(\mathcal{A},\mathcal{P},z) & \text{für } \nu=2. \end{cases}\end{aligned}$$

Wir wollen nun Bedingungen formulieren, aus denen die Ungleichungen (1) und (3) folgen:

Definition 3.6.1. Für $d|P(z)$ sei $q(d)$ der kleinste Primfaktor von $d|P(z)$. Wir setzen $q(1)=\infty$. Für $2\leq z_1\leq z$ sei

$$P_{z_1,z} = \prod_{\substack{p\in\mathcal{P}\\ z_1\leq p<z}} p = \frac{P(z)}{P(z_1)}.$$

Es sei $\mathcal{P}^{(d)} = \{p\in\mathcal{P}\colon p \not| d\}$.

Die Funktionen $\chi_\nu(d)$ für $\nu=1,2$, welche für alle $d|P(z)$ definiert sind, mögen die folgenden Bedingungen (KS) erfüllen:

Definition 3.6.2. (KS):

- (I): $\chi_\nu(d)=0$ oder $\chi_\nu(d)=1$, falls $d|P(z)$
- (II): $\chi_\nu(1)=1$
- (III): Aus $\chi_\nu(d)=1$ folgt, dass $\chi_\nu(t)=1$ für alle $t|d$ mit $d|P(z)$ (Teilergeschlossenheit).
- (IV): Aus $\chi_\nu(t)=1$, $\mu(t)=(-1)^\nu$ folgt, dass $\chi_\nu(pt)=1$ für alle $pt|P(z)$ für $p<q(t)$.

Verfahren, in denen die Siebfunktionen $S(\mathcal{A},\mathcal{P},z)$ durch die Ausdrücke

$$\sum_{d|P(z)} \mu(d)\chi_\nu(d)|\mathcal{A}_d|$$

abgeschätzt werden, heißen Kombinatorische Siebe.

Satz 3.6.1. *Die Funktionen $\chi_\nu(d)$ für $\nu=1,2$ mögen die Bedingungen (KS) aus Definition 3.6.2 erfüllen. Dann gilt*

$$\sum_{d|P(z)} \mu(d)\chi_2(d)|\mathcal{A}_d| \leq S(\mathcal{A},\mathcal{P},z) \leq \sum_{d|P(z)} \mu(d)\chi_1(d)|\mathcal{A}_d|.$$

Beweis. Mittels der Möbiusschen Umkehrformel erhalten wir

$$\sum_{d|P(z)} \mu(d)\chi_\nu(d)|\mathcal{A}_d| = \sum_{d|P(z)} |\mathcal{A}_d| \sum -\delta|d\mu\left(\frac{d}{\delta}\right)\sigma_\nu(\delta) = \sum_{\delta|P(z)} \sigma_\nu(\delta) \sum_{t|P(z)/\delta} \mu(t)|\mathcal{A}_{\delta t}|.$$

Mit

$$S(\mathcal{A},\mathcal{P},z) = \sum_{d|P(z)} \mu(d)|\mathcal{A}_d|$$

erhalten wir daraus

$$S(\mathcal{A},\mathcal{P},z) = \sum_{d|P(z)} \mu(d)\chi_\nu(d)|\mathcal{A}_d| - \sum_{1<d|P(z)} \sigma_\nu(d) S(\mathcal{A}_d,\mathcal{P}^{(d)},z). \tag{1}$$

Zur Umformung der zweiten Summe in (1) benützen wir folgende Rekursion. Für $2 \leq z_1 \leq z$ sei

$$S(\mathcal{A}, \mathcal{P}, z_1) = \sum_{t|P_{z,z}} \sum_{\substack{a \in \mathcal{A} \\ (a,P(z_1))=1 \\ (a,P_{z_1,z})=t}} 1 = \sum_{t|P_{z_1,z}} \sum_{\substack{a \in \mathcal{A}_t \\ (a,P(z)/t)=1}} 1 = \sum_{t|P_{z_1,z}} S(\mathcal{A}_t, \mathcal{P}^{(t)}, z). \tag{2}$$

Weiter haben wir

$$\sigma_\nu(\delta) = \sum_{l|\delta/q(\delta)} \mu(l)\chi_\nu(l) + \sum_{l|\delta/q(\delta)} \mu(q(\delta)l)\chi - \nu(q(\delta)l) = \sum_{l|\delta/q(\delta)} \mu(l) \cdot (\chi_\nu(l) - \chi_\nu(q(\delta)l)) \,. \tag{3}$$

Zur Behandlung der zweiten Summe in (1) setzen wir $d = q(d) \cdot \delta$ und $q(\delta) = p$. Aus der Definition von $q(\delta)$ ergibt sich dann die Bedingung $p < q(\delta)$. Mit (3) erhalten wir

$$\begin{aligned}
\sum_{1<d|P(z)} \sigma_\nu(d) S(\mathcal{A}_d, \mathcal{P}^{(d)}, z) &= \sum_{\delta|P(z)} \sum_{\substack{p|P(z) \\ p<q(\delta)}} A(\mathcal{A}_{p\delta}, \mathcal{P}^{(p\delta)}, z) \sum_{l|\delta} \mu(l) \cdot (\chi(l) - \chi(pl)) \\
&\underset{\delta=lt}{=} \sum_{l|P(z)} \sum_{\substack{p|P(z) \\ p<q(l)}} \mu(l) \cdot (\chi(l) - \chi(pl)) \cdot \sum_{\substack{t|P(z)/l \\ p<q(t)}} S(\mathcal{A}_{plt}, \mathcal{P}^{(plt)}, z) \\
&= \sum_{l|P(z)} \sum_{\substack{p|P(z) \\ p<q(l)}} \mu(l) \cdot (\chi(l) - \chi(pl)) \cdot S(\mathcal{A}_{pl}, \mathcal{P}^{(pl)}, p),
\end{aligned}$$

wobei im letzten Schritt die Rekursion (2) benutzt wurde.
Damit ergibt sich aus (1)

$$S(\mathcal{A}, \mathcal{P}, z) = \sum_{d|P(z)} \mu(d)\chi_\nu(d)|\mathcal{A}_d| - \sum_{d|P(z)} \sum_{\substack{p|P(z) \\ p<q(d)}} \mu(d) \cdot (\chi_\nu(d) - \chi_\nu(pd)) \cdot S(\mathcal{A}_{pd}, \mathcal{P}, p).$$

Dabei kann die Menge $\mathcal{P}^{(pd)}$, die sich aus dem vorigen Schritt ergibt, kann hier durch $\mathcal{P}$ ersetzt werden, da die Elemente dieser Mengen, die kleiner als p sind, dieselben sind.
Wir können nun den Beweis beenden, indem wir zeigen, dass

$$(-1)^\nu \mu(d) \cdot (\chi_\nu(d) - \chi - \nu(pd)) \leq 0 \tag{4}$$

für $\nu = 1, 2$ und für alle Paare (p, d) mit $p, d|P(z)$ und $p < q(d)$ gilt.
Dafür betrachten wir folgende Fälle:

- <u>Fall 1:</u> $\mu(d) = -(-1)^\nu$:
  Wegen der Eigenschaft (III) von χ_ν, der Teilerabgeschlossenheit, folgt $\chi_\nu(d) - \chi_\nu(pd) \geq 0$, da aus $\chi_\nu(pd) = 1$ auch $\chi - \nu(d) = 1$ folgt. Damit gilt (4).
- <u>Fall 2:</u> $\mu(d) = (-1)^\nu$:
  Wegen der Eigenschaft (IV) folgt aus $\chi_\nu(d) = 1$ auch $\chi_\nu(pd) = 1$ für $p < q(d)$. Damit gilt (4).

Damit ist der Beweis komplett. □

Satz 3.6.2. *Die Funktionen $\chi_\nu(d)$ für $\nu = 1, 2$ mögen die Bedingungen (KS) aus Definition 3.6.2 erfüllen. Dann gilt*

$$\sum_{d|P(z)} \mu(d)\chi_\nu(d)\frac{\omega(d)}{d} = W(z) \cdot \left(1 + (-1)^{\nu-1} \cdot \sum_{p<z} \frac{\omega(p)}{p} \frac{W(p)}{W(z)} \sum_{t|\mathcal{P}_{p^+,z}} \frac{\chi_\nu(t) \cdot (1 - \chi_\nu(pt)}{t} \omega(t)\right),$$

wobei hier p^+ die Primzahl $p^+ \in \mathcal{P}$ bedeute, die auf $p \in \mathcal{P}$ folgt.

Beweis. Wir zeigen zunächst:

$$\chi_\nu(t) = -\chi_\nu(pt) = (-1)^{\nu-1}\mu(t)\chi_\nu(t)\cdot(1-\chi_\nu(pt)), \tag{1}$$

falls $pt|P(z)$ und $p < q(t)$ für $\nu = 1, 2$ ist.
Fall 1: $\chi_\nu(pt) = 1$
Dann gilt wegen der Teilerabgeschlossenheit (III) auch $\chi - \nu(t) = 1$, womit (1) gilt.
Fall 2: $\chi_\nu(pt) = 0$
Dann ist (1) erfüllt, falls $\chi_\nu(t) = 0$ gilt.
Es sei nun $\chi_\nu(t) = 1$. Dies ist nach (KS) nur möglich, falls $\mu(t) = (-1)^{\nu-1}$ ist. Auch hier ist (1) erfüllt.

Wir zeigen nun als nächstes:

$$\sum_{p|d}\left(\chi_\nu((d, P_{p^+,z})) - \chi_\nu((d, P_{p,z}))\right) = 1 - \chi_\nu(d). \tag{2}$$

Es sei $d = p_1 \cdots p_r$ mit $p_1 < \ldots < p_r$. Weiter ist $(d, P_{p^+,z}) = (d, P_{p,z})$ außer für $p \in \{p_1, \ldots, p_r\}$. In diesem Fall ist $(d, P_{p_i,z}) = p_1 p_{i+1} \cdots p_r$ und $(d, P_{p_i^+,z}) = p_{i+1} \cdots p_r$. Damit haben wir

$$\begin{aligned}\sum_{p|d}\left(\chi_\nu((d, P_{p^+,z})) - \chi_\nu((d, P_{p,z}))\right) &= \chi_\nu(p_2 \cdots p_r) - \chi_\nu(p_1 \cdots p_r) + \chi_\nu(p_3 \cdots p_r) - \chi_\nu(p_2 \cdots p_r) \\ &\quad + \ldots + \chi_\nu(p_r) - \chi_\nu(p_{\nu-1} \cdot p_r) + 1 - \chi_\nu(p_r) = 1 - \chi_\nu(d),\end{aligned}$$

womit (2) gezeigt ist.
Wir setzen nun (2) in die linke Seite der Behauptung ein und erhalten

$$\sum_{d|P(z)} \mu(d)\chi_\nu(d)\frac{\omega(d)}{d} = \underbrace{W(z)}_{d=1} + \sum_{d|P(z)}\sum_{p|d}\mu\left(\frac{d}{p}\right)\left(\chi_\nu((d, P_{p^+,z})) - \chi_\nu((d, P_{p,z}))\right)\frac{\omega(d)}{d}.$$

Setze $d = \delta pt$ mit $\delta|P(p)$ und $t|P_{p^+,z}$. Damit erhalten wir

$$\begin{aligned}\sum_{d|P(z)} \mu(d)\chi_\nu(d)\frac{\omega(d)}{d} &= W(z) + \sum_{p<z}\frac{\omega(p)}{p}\sum_{\delta|P(p)}\mu(\delta)\frac{\omega(\delta)}{\delta}\sum_{t|P_{p^+,z}}\mu(t)\frac{\chi_\nu(t) - \chi_\nu(pt)}{t}\omega(t) \\ &= W(z) + (-1)^{\nu-1}\sum_{p<z}\frac{\omega(p)}{p}W(p)\sum_{t|P_{p^+,z}}\frac{\chi_\nu(t)(1-\chi_\nu(pt))}{t}\omega(t),\end{aligned}$$

wobei (1) im letzten Schritt benutzt wurde. □

3.7 Das Brunsche Sieb

Nachdem Viggo Brun das Reine Brunsche Sieb entwickelt hat, baute er in den folgenden Jahren die Methode weiter aus und erhielt das noch leistungsfähigere Brunsche Sieb. Wie das Sieb des Erathosthenes und das Reine Brunsche Sieb ist auch das Brunsche Sieb ein Kombinatorisches Sieb und erfüllt die Definition 3.6.2.
Wir beschreiben als erstes die Wahl der charakteristischen Funktionen χ_ν für $\nu = 1, 2$. Hier werden nicht nur Forderungen über die Anzahl $\nu(d)$ der Primfaktoren von $d|P(z)$ erhoben ($\nu(d) \leq 2s + 1$ bzw. $\nu(d) \leq 2s$) wie beim Reinen Brunschen Sieb, sondern auch Forderungen über die Anzahl der Primfaktoren von d in gewissen Intervallen.

Definition 3.7.1. Es sei $z \geq 2$, und (z_n) sei eine Folge mit $2 = z_r < z_{r-1} < \ldots < z_1 < z_0 = z$ für $0 \leq n < r$. Diese Folge wird später speziell gewählt werden. Es sei $b \in \mathbb{N}$. Dann setzen wir für $\nu = 1, 2$

$$\chi_\nu(d) = \begin{cases} 1, & \text{falls } \nu((d, P_{z_n,z})) \leq 2b - \nu + 2n - 1,\ 1 \leq n \leq r \\ 0 & \text{sonst.} \end{cases} \qquad (*)$$

Wir zeigen zunächst, dass mit dieser Wahl ein Kombinatorisches Sieb vorliegt.

Lemma 3.7.1. *Die Funktionen χ_ν erfülllen die Bedingungen (KS) von Definition 3.6.2.*

Beweis. Die Gültigkeit von (I) bis (III) ist unmittelbar klar. Wir wollen die Gültigkeit von (IV) beweisen.
Es sei $\nu(t) = (-1)^\nu$, $p < q(t)$ und $z_m \leq p < z_{m-1}$. Um $\chi_\nu(pt) = 1$ zu zeigen, genügt es, die Gültigkeit von $(*)$ für $n = m$ nachzuweisen, also die Ungleichung $\nu(pt) \leq 2b - \nu + 2m - 1$. Wegen $\chi_\nu(t) = 1$ ist $\nu(t) \leq 2b - \nu + 2m - 1$. Wegen $\mu(t) = (-1)^{\nu(t)} = (-1)^\nu$ ist $\nu(t) = 2b - \nu + 2m - 1$ nicht möglich. Damit gilt $\nu(t) < 2b - \nu + 2m - 1$ und $\nu(pt) \leq 2b - \nu + 2m - 1$, womit auch (IV) gezeigt ist. □

Zur Formulierung eines allgemeinen Ergebnisses führen wir noch eine weitere Bedingung über die multiplikative Funktion ω und die Reste R_d ein.

Definition 3.7.2. Es sei $\kappa > 0$, $A_0' \geq 1$, $A_2 \geq 1$, $L \geq 1$ und $0 < \alpha \leq 1$. Dann ist die Bedingung $(\Omega_2(\kappa))$ durch

$$\sum_{w \leq p < z} \frac{\omega(p) \log p}{p} \leq \kappa \log \frac{z}{w} + A_2 \qquad (\Omega_2(\kappa))$$

für $2 \leq w \leq z$ gegeben.
Die Bedingungen (R_0) und $(R_1(\kappa, \alpha))$ sind durch

$$|R_d| \leq L \cdot \left(\frac{X \log X}{d} + 1 \right) \cdot A_0'^{\nu(d)} \qquad (R_0)$$

für $\nu(d) \neq 0$ und $p|d \Rightarrow p \in \mathcal{P}$ sowie, dass für jedes $u \geq 1$ ein $C_0 > 0$ mit

$$\sum_{\substack{d < X^\alpha \log^{-C_0} X \\ p|d \Rightarrow p \in \mathcal{P}}} \mu^2(d) |R_d| = O_u\left(\frac{X}{\log^{\kappa+u} X} \right) \qquad (R_1(\kappa, \alpha))$$

existiert, gegeben.

Bemerkung 3.7.1. Aus dem Ergebnis von Satz 2.3.2

$$\sum_{p < z} \frac{\log p}{p} = \log z + O(1)$$

sieht man, dass die Bedingung $(\Omega_2(\kappa))$ folgendes besagt:
In jedem nicht zu kurzen Intervall $[w, z]$ ist der durchschnittliche Wert dieser Funktion $\omega(p)$ kleiner gleich κ.

In manchen Aussagen der Siebtheorie treten auch zweiseitige Bedingungen der Form

$$-L \leq \sum_{w \leq p < z} \frac{\omega(p) \log p}{p} - \kappa \log \frac{z}{w} \leq A_2 \qquad (\Omega_2(\kappa, L))$$

auf. Dann ist κ der durchschnittliche Wert von $\omega(p)$. Man nennt κ die Dimension des Siebs. Für $\kappa = 1$ spricht man von einem linearen Sieb.

Zur Vorbereitung des Hauptresultats benötigen wir

Lemma 3.7.2. (Ω_1), $(\Omega_2(\kappa))$
Für $2 \le w \le z$ haben wir

$$\frac{W(w)}{W(z)} \le \exp\left(\kappa \log\frac{\log z}{\log w} + \frac{A_2}{\log w}\cdot\left(1 + A_1\kappa + \frac{A_1 A_2}{\log 2}\right)\right).$$

Beweis. Nach $(\Omega_2(\kappa, L))$ gilt

$$\sum_{w\le p<z} \frac{\omega(p)\log p}{p} \le \kappa \log\frac{z}{w} + A_2,$$

woraus mit partieller Summation

$$\begin{aligned}
\sum_{w\le p<z}\frac{\omega(p)}{p} &\le \frac{\kappa\log\frac{z}{w}+A_2}{\log z} + \int_w^z \frac{\kappa\frac{t}{w}+A_2}{t\log^2 t}\,dt \\
&= \frac{\kappa(\log z - \log w)+A_2}{\log z} + \int_w^z \frac{\kappa(\log t - \log w)+A_2}{t\log^2 t}\,dt \\
&= \kappa - \kappa\frac{\log w}{\log z} + \frac{A_2}{\log z} + \kappa\cdot\int_w^z \frac{dt}{t\log t} + (-\kappa\log w + A_2)\cdot\int_w^z \frac{dt}{t\log^2 t} \\
&= \kappa - \kappa\frac{\log z}{\log w} + \frac{A_2}{\log z} + \kappa\log\frac{\log z}{\log w} + (-\kappa\log w + A_2)\cdot\left(-\frac{1}{\log z}+\frac{1}{\log w}\right) \\
&= \kappa\log\frac{\log z}{\log w} + \frac{A_2}{\log w}
\end{aligned}$$

folgt. Also gilt

$$\sum_{w\le p<z}\frac{\omega(p)}{p} \le \kappa\log\frac{\log z}{\log w} + \frac{A_2}{\log w}. \tag{1}$$

Ebenfalls durch partielle Summation erhalten wir aus $(\Omega_2(\kappa))$:

$$\begin{aligned}
\sum_{e\le p<z}\frac{\omega(p)}{p\log p} &\le \frac{\kappa\log\frac{z}{w}+A_2}{\log^2 z} + 2\cdot\int_w^z \frac{\kappa\log\frac{t}{w}+A_2}{t\log^3 t}\,dt \\
&= \frac{\kappa}{\log z} - \kappa\cdot\frac{\log w}{\log^2 z} + \frac{A_2}{\log^2 z} + 2\kappa\cdot\left(-\frac{1}{\log z}+\frac{1}{\log w} - \log w\cdot\left(\frac{1}{2\log^2 w}-\frac{1}{2\log^2 z}\right)\right) \\
&\quad +2A_2\cdot\left(\frac{1}{2\log^2 w}-\frac{1}{2\log^2 z}\right) \\
&= -\frac{2\kappa}{\log z} + \frac{\kappa}{\log w} + \kappa\cdot\frac{\log w}{\log^2 z} + \frac{A_2}{\log^2 w} \le \frac{1}{\log w}\cdot\left(\kappa + \frac{A_2}{\log w}\right).
\end{aligned}$$

Also gilt

$$\sum_{w\le p<z}\frac{\omega(p)}{p\log p} \le \frac{1}{\log w}\cdot\left(\kappa + \frac{A_2}{\log w}\right). \tag{2}$$

Die Wahl $w = p$ und $z = p + \epsilon$ in $(\Omega_2(\kappa))$ führt zu

$$\frac{\omega(p)}{p\log p} \le A_2. \tag{3}$$

Aus (Ω_1), also $0 \le \frac{\omega(p)}{p} \le 1 - \frac{1}{A_1}$ folgt

$$g(p) := \frac{\omega(p)}{p\cdot\left(1-\frac{\omega(p)}{p}\right)} \le A_1\cdot\frac{\omega(p)}{p}. \tag{4}$$

Aus (2), (3) und (4) erhalten wir

$$\sum_{w\le p<z}\frac{\omega(p)}{p}\le A_1A_2\cdot\sum_{w\le p<z}\frac{\omega(p)}{p\log p}\le\frac{A_1A_2}{\log w}\cdot\left(\kappa+\frac{A_2}{\log w}\right). \tag{5}$$

Es ist $g(p)=\frac{\omega(p)}{p}+\frac{\omega(p)}{p}\cdot g(p)$. Daraus und aus (1) und (5) erhalten wir

$$\sum_{w\le p<z}g(p)\le\kappa\cdot\log\frac{\mathrm{Log}z}{\log w}+\frac{A_2}{\log w}+\frac{A_1A_2}{\log w}\cdot\left(\kappa+\frac{A_2}{\log w}\right). \tag{6}$$

Es ist

$$\begin{aligned}\frac{W(w)}{W(z)} &= \frac{1}{\prod_{w\le p<z}\left(1-\frac{\omega(p)}{p}\right)}=\prod_{w\le p<z}(1+g(p))\le\exp\left(\sum_{w\le p<z}g(p)\right)\\ &\le \exp\left(\kappa\cdot\log\frac{\log z}{\log w}+\frac{A_2}{\log w}\cdot\left(1+A_1\kappa+\frac{A_1A_2}{\log z}\right)\right).\end{aligned}$$

Dies beweist Lemma 3.7.2. □

Satz 3.7.1. *(Brunsches Sieb):* (Ω_1), $(\Omega_2(\kappa))$, (R_0), $(R_1(\kappa,\alpha))$
Es seien $b\in\mathbb{N}$, $\lambda\in\mathbb{R}$ *mit* $0<\lambda e^{1+\lambda}<1$, $c_1=\frac{A_2}{2}\cdot\left(1+A_1\kappa+\frac{A_1A_2}{\log 2}\right)$ *und* $u=\frac{\log X}{\log z}$.
Dann gilt

$$\begin{aligned}S(\mathcal{A},\mathcal{P},z) &\le XW(z)\cdot\left(1+2\cdot\frac{\lambda^{2b+1}e^{2\lambda}}{1-\lambda^2e^{2+2\lambda}}\exp\left((2b+3)\cdot\frac{c_1}{\lambda\log z}\right)\right.\\ &\quad\left.+O\left(Lz^{-\alpha u+2b+\frac{2{,}01}{e^{\frac{2\lambda}{\kappa}}-1}}u^{C_0+1}\log^{C_0+\kappa+1}z\right)+O_u\left(u^{-\kappa}\log^{-u}X\right)\right)\end{aligned}$$

und

$$\begin{aligned}S(\mathcal{A},\mathcal{P},z) &\ge XW(z)\cdot\left(1-2\cdot\frac{\lambda^{2b}e^{2\lambda}}{1-\lambda^2e^{2+2\lambda}}\exp\left((2b+2)\cdot\frac{c_1}{\log z}\right)\right.\\ &\quad\left.+O\left(Lz^{-\alpha u+2b-1+\frac{2{,}01}{e^{\frac{2\lambda}{\kappa}}-1}}u^{C_0+1}\log^{C_0+\kappa+1}z\right)+O_u\left(u^{-\kappa}\log^{-u}X\right)\right).\end{aligned}$$

Die O- Konstanten können von A_0', A_1, A_2, κ *und* u *abhängen. Sie hängen nicht von* λ *oder* b *ab.*

Beweis. Da wir für die in den O- Symbolen implizierten Konstanten beliebig große, aber feste Werte annehmen dürfen, können wir in der Folge annehmen, dass

$$z\ge B \tag{1}$$

mit einer festen, aber beliebig großen Konstanten B ist. Es sei

$$\Lambda=\frac{2\pi}{\kappa}\cdot\frac{1}{1+\epsilon}\quad\text{mit}\quad\epsilon=\frac{1}{200\epsilon^{1/\kappa}}. \tag{2}$$

Wir definieren dann die Folge (z_n) durch

$$\log z_n=e^{-n\Lambda}\log z \tag{3}$$

für $n=1,\dots,r-1$ und $z_r=2$.

Dabei wird r so gewählt, dass

$$\log z_{r-1} = e^{-(r-1)\Lambda} \log z > \log 2$$

und

$$e^{-r\Lambda} \log z \leq \log 2,$$

so dass

$$e^{(r-1)\Lambda} < \frac{\log z}{\log 2} \leq e^{r\Lambda} \tag{4}$$

gilt. Dann ist die Bedingung von Definition 3.7.1

$$2 = z_r < z_{r-1} < \ldots < z_1 < z_0 = z$$

erfüllt. Die Funktionen $\chi_\nu(d)$ für $\nu = 1, 2$ seien durch die Definition 3.7.1 gegeben. Nach Lemma 3.7.1 sind die Bedingungen (KS) des Kombinatorischen Siebs erfüllt, und wir haben nach Satz 3.6.1

$$\sum_{d|P(z)} \mu(d)\chi_2(d)|\mathcal{A}_d| \leq S(\mathcal{A}, \mathcal{P}, z) \leq \sum_{d|P(z)} \mu(d)\chi_1(d)|\mathcal{A}_d|. \tag{5}$$

Wie in früheren Sieben benützen wir die Approximation

$$|\mathcal{A}_d| = \frac{\omega(d)}{d} X + R_d$$

und behandeln die Beiträge der Hauptglieder

$$X \sum\nolimits_H^{(r)} \quad \text{mit} \quad X \sum\nolimits_H^{(r)} = \sum_{d|P(z)} \mu(d)\chi^{(r)}(d)\frac{\omega(d)}{d} \tag{6}$$

und den Restgliedern

$$X \sum\nolimits_R^{(r)} = \sum_{d|P(z)} \mu(d)\chi^{(r)}(d)R_d \tag{7}$$

getrennt.
Nach Satz 3.6.2 haben wir

$$\sum_{d|P(z)} \mu(d)\chi_\nu(d)\frac{\omega(d)}{d} = W(z) \cdot \left(1 + (-1)^{\nu-1} \cdot \sum_{p<z} \frac{\omega(p)}{p}\frac{W(p)}{W(z)} \sum(p)\right) \tag{8}$$

mit

$$\sum(p) := \sum_{t|P_{p^+,z}} \frac{\chi_\nu(z) \cdot (1 - \chi_\nu(pt))}{t}\omega(t). \tag{9}$$

Es ist

$$\begin{aligned} \sum_{p<z} \frac{\omega(p)}{p}\frac{W(p)}{W(z)} \sum(p) &\leq \sum_{n=1}^{r} \sum_{z_n \leq p < z_{n-1}} \frac{\omega(p)}{p}\frac{W(p)}{W(z)} \sum_{t|P_{p^+,z}} \frac{\chi_\nu(z) \cdot (1 - \chi_\nu(pt))}{t}\omega(t) \\ &\leq \sum_{n=1}^{r} \frac{W(z_n)}{W(z)} \sum_{z_n \leq p < z_{n-1}} \frac{\omega(p)}{p} \sum_{t|P_{p^+,z}} \frac{\chi_\nu(z) \cdot (1 - \chi_\nu(pt))}{t}\omega(t) \end{aligned}$$

wegen $W(p) \leq W(Z_n)$ für $z_n \leq p < z_{n-1}$.

Es ist nur dann $\chi_\nu(t) \cdot (1 - \chi_\nu(pt)) \neq 0$, wenn $\chi_\nu(t) = 1$ und $\chi_\nu(pt) = 0$ ist, woraus wegen (IV) von (KS) dann $\nu(t) = 2b - \nu + 2n - 1$ folgt. Daraus folgt

$$\sum_{p<z} \frac{\omega(p)}{p} \frac{W(p)}{W(z)} \sum(p) \underset{1=p\cdot t}{\leq} \sum_{n=1}^{r} \frac{W(z_n)}{W(z)} \sum_{\substack{d|P_{z_n,z} \\ \nu(d)=2b-\nu+2n}} \frac{\omega(d)}{d}.$$

Mit

$$\sum_{d|P_{z_n,z}} \frac{\omega(d)}{d} \leq \frac{1}{(2b-\nu+2n)!} \cdot \left(\sum_{z_n \leq p < z} \frac{\omega(p)}{p} \right)^{2b-\nu+2n}$$

erhalten wir

$$\sum_{p<z} \frac{\omega(p)}{p} \frac{W(p)}{W(z)} \sum(p) \leq \sum_{n=1}^{r} \frac{W(z_n)}{W(z)} \cdot \frac{1}{(2b-\nu+2n)!} \cdot \left(\sum_{z_n \leq p < z} \frac{\omega(p)}{p} \right)^{2b-\nu+2n}. \tag{10}$$

Wir setzen

$$c := \frac{c_1}{\log z} \tag{11}$$

und zeigen im folgenden

$$\frac{W(z_n)}{W(z)} \leq e^{2(n\lambda+c)} \tag{12}$$

für $n = 1, \ldots, r$. Nach Lemma 3.7.2 haben wir

$$\begin{aligned} \frac{W(z_n)}{W(z)} &\leq \exp\left(\kappa \log \frac{\log z}{\log z_n} + \frac{A_2}{\log z_n} \cdot \left(1 + A_1\kappa + \frac{A_1 A_2}{\log 2} \right) \right) \\ &= \exp\left(n\Lambda\kappa + \frac{2c_1 e^{n\Lambda}}{\log z} \right) = e^{2c} \cdot \exp\left(n \cdot \left(\Lambda\kappa + \frac{2c_1}{\log z} \cdot \frac{e^{n\Lambda}-1}{n} \right) \right), \end{aligned}$$

also

$$\frac{W(z_n)}{W(z)} \leq e^{2c} \cdot \exp\left(n \cdot \left(\Lambda\kappa + \frac{2c_1}{\log z} \cdot \frac{e^{n\Lambda}-1}{n} \right) \right) \tag{13}$$

für $n = 1, \ldots, r-1$. Die Ungleichung (13) gilt auch für $n = r$, da aus (4) die Aussage

$$\frac{\log z}{\log z_n} = \frac{\log z}{\log 2} \leq r\Lambda\kappa$$

folgt. Wegen $\Lambda > 0$ haben wir

$$\frac{e^{n\Lambda}-1}{n} \leq \frac{e^{r\Lambda}-1}{r}.$$

Nach (13) ist

$$\frac{e^{r\Lambda}-1}{r} \leq \Lambda \cdot \frac{e^{r\Lambda}}{r\Lambda} \leq \Lambda \cdot \frac{e^{\Lambda}}{\log 2} \cdot \frac{\log z}{\log \frac{\log z}{\log 2}}.$$

Deshalb erhalten wir aus (13)

$$\frac{W(z_n)}{W(z)} \leq e^{2c} \cdot \exp\left(n\Lambda\kappa \cdot \left(1 + \frac{2c_1 e^{\Lambda}}{\kappa \log 2} \cdot \frac{1}{\log \frac{\log z}{\log 2}} \right) \right)$$

Wegen $z \geq B$ haben wir

$$\frac{W(z_n)}{W(z)} \leq e^{2(n\lambda+c)}$$

für $n = 1, \ldots, r$, also (12).

Wegen (10) und (12) erhalten wir

$$\sum(p) \le \sum_{n=1}^{r} e^{2n\lambda+c} \cdot \left(\sum_{z_n \le p < z} \frac{\omega(p)}{p} \right)^{2b-\nu+2n}.$$

Wegen

$$\sum_{z_n \le p < z} \frac{\omega(p)}{p} \le \sum_{z_n \le p < z} \log \frac{1}{1 - \frac{\omega(p)}{p}} = \log \frac{W(z_n)}{W(z)}$$

und wegen $(2b-\nu+2n)! \ge (2n)!(2n)^{2b-\nu}$ erhalten wir

$$\begin{aligned}
\sum_{p<z} \frac{\omega(p)}{p} \frac{W(p)}{W(z)} \sum(p) &\le \sum_{n=1}^{r} e^{2n\lambda+2c} \cdot \frac{(2n\lambda+2c)^{2b-\nu+2n}}{(2b-\nu+2n)!} \\
&\le e^{2c} \cdot \sum_{n=1}^{r} e^{2n\lambda} \cdot \frac{(2n\lambda+2c)^{2b-\nu} \cdot (2n\lambda+2c)^{2n}}{(2n)!(2n)^{2b-\nu}} \\
&= e^{2c} \cdot \sum_{n=1}^{r} e^{2n\lambda} \cdot \frac{\left(\lambda + \frac{c}{n}\right)^{2b-\nu} \cdot (2n\lambda+2c)^{2n}}{(2n)!} \\
&\le e^{2c} \cdot (\lambda+c)^{2b-\nu} \cdot \sum_{n=1}^{r} \frac{\left(\lambda + \frac{c}{n}\right)^{2b-\nu} \cdot (2n\lambda+2c)^{2n}}{(2n)!} \\
&\le e^{2c} \cdot (\lambda+c)^{2b-\nu} \cdot \sum_{n=1}^{r} \frac{\lambda^{2n} \cdot (2ne^{-1})^{2n}}{(2n)!} \cdot \left(1 + \frac{c}{n\lambda}\right)^{2n} \cdot \left(e^{1+\lambda}\right)^{2n}.
\end{aligned}$$

Die Folge $(ne^{-1})^n/n!$ ist in n monoton fallend, und es gilt $\left(1 + \frac{c}{n\lambda}\right)^{2n} \le e^{2c/\lambda}$. Damit haben wir

$$\begin{aligned}
\sum_{p<z} \frac{\omega(p)}{p} \frac{W(p}{W(z)} \sum(p) &\le e^{2c} \cdot (\lambda+c)^{2b-\nu} 2e^{-2} e^{2c/\lambda} \cdot \sum_{n=1}^{\infty} \left(\lambda e^{1+\lambda}\right)^{2n} \\
&= \frac{2\lambda^{2b-\nu+2}}{1-\lambda^2 e^{2+2\lambda}} \cdot \left(1 + \frac{c}{\lambda}\right)^{2b-\nu} \cdot e^{2c(1+1/\lambda)} \le 2\frac{\lambda^{2b-\nu+2} e^{2\lambda}}{1-\lambda^2 e^{2+2\lambda}} \cdot e^{(2b-\nu+4)c/\lambda},
\end{aligned}$$

also

$$\sum_{p<z} \frac{\omega(p)}{p} \frac{W(p}{W(z)} \sum(p) \le 2\frac{\lambda^{2b-\nu+2} e^{2\lambda}}{1-\lambda^2 e^{2+2\lambda}} \cdot e^{(2b-\nu+4)c/\lambda}. \tag{14}$$

Aus (8) und (14) folgt nun

$$\begin{aligned}
\sum_{d|P(z)} \mu(d)\chi_\nu(d) \frac{\omega(d)}{d} &= W(z) \cdot \left(1 + \theta \cdot 2\frac{\lambda^{2b-\nu+2} e^{2\lambda}}{1-\lambda^2 e^{2+2\lambda}} \cdot e^{(2b-\nu+4)c/\lambda}\right) \\
&= W(z) \cdot \left(1 + \theta \cdot 2\frac{\lambda^{2b-\nu+2}}{1-\lambda^2 e^{2+2\lambda}} \cdot \exp\left((2b+3) \cdot \frac{c_1}{\log z}\right)\right)
\end{aligned}$$

für $\nu = 1, 2$, also

$$\sum_{d|P(z)} \mu(d)\chi_\nu(d) \frac{\omega(d)}{d} = W(z) \cdot \left(1 + \theta \cdot 2\frac{\lambda^{2b-\nu+2}}{1-\lambda^2 e^{2+2\lambda}} \cdot \exp\left((2b+3) \cdot \frac{c_1}{\log z}\right)\right). \tag{15}$$

Wir kommen nun zur Behandlung des Beitrages der Restglieder:
Wir beginnen mit der Summe

$$\sum_{d|P(z)} \chi_\nu(d) A^{\nu(d)}$$

für eine Konstante $A \geq 1$. Es gilt

$$\sum_{d|P(z)} \chi_\nu(d) A^{\nu(d)} \leq \left(1 + \sum_{p<z} A\right)^{2b-\nu+1} \prod_{n=1}^{r-1} \left(1 + \sum_{p<z} A\right)^2,$$

wie man durch Ausmultiplizieren der rechten Seite überprüft.
Anwendung der Tschebyschewschen Schranke

$$\pi(z) \leq \frac{2z}{\log z} + b$$

mit einer geeigneten Konstanten b ergibt

$$\sum_{d|P(z)} \chi_\nu(d) A^{\nu(d)} \leq \left(1 + A \cdot \left(\frac{2z}{\log z} + 3\right)^{2b-\nu+1}\right) \cdot \prod_{n=1}^{r-1} \left(1 + A \cdot \left(\frac{2z}{\log z} + 3\right)\right)^2.$$

Damit erhalten wir für hinreichend große C

$$\sum_{d|P(z)} \chi_\nu(d) A^{\nu(d)} \leq \left(\frac{Cz}{\log z}\right)^{2b-\nu+1} \prod_{n=1}^{r-1} \left(\frac{Cz_n e^{n\Lambda}}{\log z}\right)^2. \tag{16}$$

Es ist

$$\prod_{n=1}^{r-1} \left(\frac{Ce^{n\Lambda}}{\log z}\right) = \left(\frac{B^{r\Lambda/2}}{\log z}\right)^{r-1}$$

und wegen

$$e^{r-1/\Lambda} < \frac{\log z}{\log 2} \leq e^{r\Lambda}$$

auch

$$\frac{Be^{r\Lambda/2}}{\log z} \leq \frac{Be^{\Lambda/2}}{\log z} \cdot \left(\frac{\log z}{\log 2}\right)^{1/2} < 1. \tag{17}$$

Weiter ist

$$\prod_{n=1}^{r-1} z_n^2 = \exp\left(2 \log z \cdot \sum_{n=1}^{r-1} e^{-n\Lambda}\right) \leq z^{\frac{2}{e^\Lambda - 1}}. \tag{18}$$

Aus (16), (17) und (18) folgt

$$\sum_{d|P(z)} \chi_\nu(d) A^{\nu(d)} = O\left(z^{2b-\nu+1+\frac{2}{e^\Lambda-1}}\right).$$

Es ist

$$e^{2\lambda/\kappa} - e^\Lambda \leq \left(\frac{2\lambda}{\kappa} - \Lambda\right) \cdot e^{2\lambda/\kappa} \leq \epsilon^\Lambda \cdot e^{1/\kappa},$$

und wegen $e^\Lambda - 1 \geq \Lambda$ folgt

$$\frac{e^{2\lambda/\kappa}}{e^\Lambda - 1} \leq 1 + \frac{\epsilon\Lambda e^{1/\kappa}}{e^\Lambda - 1} \leq 1 + \epsilon \cdot e^{1/\kappa} = \frac{2,01}{2}.$$

Damit folgt

$$\sum_{d|P(z)} \chi_\nu(d) A^{\nu(d)} = O\left(z^{2b+1-\nu+\frac{2,01}{e^{2\lambda/\kappa}-1}}\right) \tag{19}$$

für $\nu = 1, 2$. Aus (19) folgt nun

$$\begin{aligned}
\sum_{d|P(z)} \chi_\nu(d)|R_d| &\leq \sum_{\substack{d<X^\alpha \log^{-C_0} X \\ p|d \Rightarrow p\in\mathcal{P}}} |R_d| + L \cdot \sum_{\substack{d|P(z) \\ d\geq X^\alpha \log^{-C_0} X}} \left(\frac{X\log X}{d}+1\right) \cdot A_0'^{\nu(d)} \chi_\nu(d) \\
&\leq O_u\left(\frac{X}{\log^{\kappa+u} X}\right) + 2LX^{1-\alpha}\log^{C_0+1} X \cdot \sum_{d|P(z)} A_0'^{\nu(d)}\chi_\nu(d) \\
&= O_u\left(\frac{X}{\log^{\kappa+u} X} + LX^{1-\alpha} z^{2b+1-\nu+(2,01/e^{2\lambda/\kappa}-1)} \log^{C_0+1} X\right).
\end{aligned}$$

Also gilt

$$\sum_{d|P(z)} \chi_\nu(d)|R_d| = O\left(\frac{u^{-\kappa}}{\log^u X} + Lz^{-\alpha u+2b+1-\nu+\frac{2,01}{e^{\frac{2\lambda}{\kappa}}-1}} u^{C_0+1}\log^{C_0+\kappa+1} z\right)$$

für $\nu = 1, 2$. □

Wir schließen diesen Abschnitt mit zwei Anwendungen:

Satz 3.7.2. *Es gibt unendlich viele natürliche Zahlen n, für die sowohl n als auch $n+2$ höchstens sieben Primfaktoren haben.*

Lemma 3.7.3. *Es gibt Konstanten λ und u mit $0 < \lambda e^{1+\lambda} < 1$,*

$$1 - \frac{2\lambda^2 e^{2\lambda}}{1-\lambda^2 e^{2+2\lambda}} > 0 \quad \textit{und} \quad 2 + \frac{2,01}{e^\lambda - 1} < u \leq 8.$$

Beweis. (Beweis von Satz 3.7.2)
Wir wenden das Brunsche Sieb (Satz 3.7.1) mit $\mathcal{A} = \{n(n+2) \colon n \leq x\}$ an.
Nach Beispiel 3.2.3 in Abschnitt 3.2 haben wir

$$|\mathcal{A}_d| = \frac{\omega(d)}{d} X + R_d$$

mit $X = x$, wobei die multiplikative Funktion ω durch $\omega(2) = 1$ und $\omega(p) = 2$ für $p > 2$ bestimmt ist. Wir haben $|R_d| \leq 2^{\nu(d)}$. Die Bedingungen (Ω_0), also $\omega(p) \leq A_0$ und (Ω_1), d.h. $0 \leq \frac{\omega(p)}{p} \leq 1 - \frac{1}{A_1}$ sind mit $A_0 = 2$ und $A_1 = 3$ erfüllt. Nach Satz 3.1.2 gilt

$$\sum_{p\leq x} \frac{\log p}{p} = \log x + O(1).$$

Somit ist die Bedingung $(\Omega_2(\kappa))$

$$\sum_{w\leq p<z} \frac{\omega(p)\log p}{p} \leq \kappa \log\frac{z}{w} + A_2$$

mit passendem A_2 für $\kappa = 2$ erfüllt.

Jedes Teilintervall von $(0, x]$ der Länge d mit $\mu^2(d) = 1$ enthält höchstens $2^{\nu(d)}$ Werte n, für die $n(n+2) \in \mathcal{A}_d$ gilt. Das Intervall $(0, x]$ kann durch $(\left[\frac{x}{d}\right] + 1)$ solcher Teilintervalle überdeckt werden.. Daher ist die Bedingung (R_0)

$$|R_d| \leq L \cdot \left(\frac{X \log X}{d} + 1\right) \cdot A_0'^{\nu(d)}$$

für $\nu(d) \neq 0$ mit $L = 1$ und $A_0' = 2$ erfüllt. Wegen $|R_d| \leq 2^{\nu(d)}$ ist die Bedingung $(R_1(\kappa, \alpha))$

$$\sum_{\substack{d < X^\alpha \log^{-C_0} X \\ p|d \Rightarrow p \in \mathcal{P}}} \mu^2(d)|R_d| = O_U\left(\frac{X}{\log^{\kappa+U} X}\right)$$

für $\alpha = 1 - \epsilon$ mit einem beliebig kleinen $\epsilon > 0$ sowie $C_0 > 0$ und $U > 0$ erfüllt.
Es ist

$$W(z) = \frac{1}{2} \prod_{2<p<z} \left(1 - \frac{2}{p}\right).$$

Mit Satz 3.7.1 und der Wahl $b = 1$ erhalten wir

$$S(\mathcal{A}, \mathcal{P}, z) \geq \frac{1}{2}x \cdot \prod_{2<p<z} \left(1 - \frac{2}{p}\right) \cdot \left(1 - 2 \cdot \frac{\lambda^{2b} e^{2\lambda}}{1 - \lambda^2 e^{2+2\lambda}} \exp\left((2b+2) \cdot \frac{c_1}{\log z}\right)\right.$$

$$\left. + O\left(L z^{-\alpha u + 2b - 1 + \frac{2,01}{e^{\frac{2\lambda}{\kappa}} - 1}} u^{C_0+1} \log^{C_0+2} z\right) + O_U\left(u^{-2} \log^{-U} x\right)\right). \tag{1}$$

Wir benutzen folgendes numerisches Resultat:
Es gibt Konstanten λ und u mit $0 < \lambda e^{1+\lambda} < 1$ sowie

$$1 - \frac{2\lambda^2 e^{2\lambda}}{1 - \lambda^2 e^{2+2\lambda}} > 0 \quad \text{und} \quad 2 + \frac{2,01}{e^\lambda - 1} < u \leq 8.$$

Wir setzen $z = x^{1/u}$. Dann strebt die rechte Seite von (1) gegen ∞ für $x \to \infty$. Es gibt somit unendlich viele n, so dass aus $p|n(n+2)$ die Aussage $p \geq n^{1/u}$ folgt.
Es sei $n = p_1 \cdots p_{\tilde{\nu}(n)}$ bzw. $n + 2 = p_1 \cdots p_{\tilde{\nu}(n+2)}$ die Zerlegung von n bzw. $n + 2$ in nicht notwendigerweise verschiedene Primfaktoren. Wegen $n \geq (n^{1/4})^{\tilde{\nu}(n)}$ und $n + 2 \geq (n+2)^{\tilde{\nu}(n+2)/n}$ folgt $\tilde{\nu}(n) \leq 7$ und $\tilde{\nu}(n+2) \leq 7$ für $n \geq n_0$ mit einem hinreichend großen n_0. □

Die obere Schranke für $\pi_2(x)$ geben wir ohne Beweis an.

Satz 3.7.3. *Es gilt*

$$\pi_2(x) = O\left(\frac{x}{\log^2 x}\right).$$

3.8 Untere Schranken für die Anzahl von paarweise orthogonalen Lateinischen Quadraten

Satz 3.8.1. *(Chowla, Erdös, Straus)*
Es gibt ein $n_0 \in \mathbb{N}$, so dass

$$N(n) \geq n^{1/91}$$

für $n \geq n_0$ gilt.

Beweis. Wir wenden Satz 2.3.4 an.
Es sei $k \leq N(m)+1$ mit $1 \leq w \leq m$. Dann gilt

$$N(km+w) \geq \min\{N(m), N(w), N(k)-1, N(k+1)-1\}.$$

Es gibt zwei Fälle:

- Fall 1: Es ist n gerade:
  Dann werden k, m und w alle ungerade gewählt.
- Fall 2: Es ist n ungerade:
  Dann wird k gerade gewählt und m und w ungerade.

Beide Fälle werden sehr ähnlich behandelt.
In einer ersten Anwendung des Brunschen Siebes bestimmen wir $k_0 \in \mathbb{N}$, so dass eine der Zahlen k_0 bzw. k_0+1 durch eine Potenz von 2^{l_0} mit $n^{\zeta_0} \leq 2^{l_0} < 2n^{\zeta_0}$ teilbar ist und keine der Zahlen k_0 bzw. k_0+1 durch eine Primzahl, die kleiner als 2^{l_0} ist, teilbar ist.
In einer zweiten Anwendung des Brunschen Siebes benützen wir die Gleichung $m = \frac{n_0-w}{k_0}$ und sieben die Menge

$$\mathcal{B} = \left\{ w \cdot \frac{n_0-w}{k_0} \colon w \equiv n \bmod k_0,\ w \in I \right\}.$$

Wir behandeln nur die Einzelheiten von Fall 1 und beschreiben dann kurz die Änderungen für Fall 2:

- 1. Schritt:
  Bestimmung von k_0:
  Wir setzen

  $$\zeta_0 := \frac{1}{90,5}. \tag{1}$$

  Wir wenden Satz 3.7.1 mit

  $$\mathcal{A} = \{h \cdot (2^{l_0}h - 1) \colon \frac{1}{2}n^{8\zeta_0} < h \leq n^{8\zeta_0}\}$$

  an und wählen $z = n^{\zeta_0}$ und $\mathcal{P} = \mathbb{P}$, $X = \frac{1}{2}n^{8\zeta_0}$ sowie

  $$\omega(p) = \begin{cases} 0 & \text{für } p = 2, \\ 2 & \text{für } p > 2. \end{cases} \tag{2}$$

  Wir überprüfen die Bedingungen von Satz 3.7.1

  - $(\Omega_0)\colon \omega(p) \leq A_0$ ist mit $A_0 = 2$ erfüllt.
  - $(\Omega_1)\colon \omega(p) \leq A_1$ ist mit $A_1 = 3$ erfüllt.
  - Wir haben

    $$(\Omega_2(\kappa))\colon \sum_{w \leq p < z} \frac{\omega(p)\log p}{p} \leq \kappa \cdot \frac{\log z}{\log w} + B$$

    mit einer passenden Konstanten $B > 0$.

  Wir kommen nun zur Diskussion der Bedingungen für die Restglieder:
  Die Kongruenz

  $$h(2^l h - 1) \equiv 0 \bmod p \tag{3}$$

  ist zu den beiden Kongruenzen

  $$h \equiv 0 \bmod p \quad \text{und} \quad 2^l h \equiv 1 \bmod p \tag{4}$$

  äquivalent. Für $p = 2$ hat (3) keine Lösung. Für $p > 2$ hat (4) die Lösungen $h \equiv 0 \bmod p$ bzw. $h \equiv (2^l)_p^{-1} \bmod p$, wobei $(2^l)_p^{-1}$ durch die Kongreunz $(2^l)_p^{-1} 2^l \equiv 1 \bmod p$ bestimmt ist.

Es sei $\epsilon > 0$ fest und beliebig klein und für

$$d \leq n^{8\zeta_0(1-\epsilon)} \tag{5}$$

enthält jedes Intervall der Länge d genau $\omega(d)$ Lösungen von

$$h(2^l h - 1) \equiv 0 \bmod d, \tag{6}$$

wobei $\omega(d)$ durch (2) und durch die Multiplikativität bestimmt ist.
Dies sieht man, indem man das System (3) von Kongruenzen modulo p nach dem Chinesischen Restsatz durch die eine Kongruenz (5) ersetzt. Aufteilen des Intervalls $(\frac{1}{2}n^{8\zeta_0}, n^{8\zeta_0})$ in Teilintervalle der Länge d zeigt, dass

$$|\mathcal{A}| = \frac{\omega(d)}{d} \cdot X + R_d$$

mit $|R_d| \leq 2^{\nu(d)}$ gilt.
Wir sehen, dass (R_0), nämlich

$$|R_d| \leq L \cdot \left(\frac{X \log X}{d} + 1 \right) \cdot A_0'^{\nu(d)}$$

mit $L = 1$, $A_0' = 2$ und $(R_1(\kappa, \alpha))$, nämlich

$$\sum_{\substack{d < X^\alpha \log^{-C_0} X \\ p|d \Rightarrow p \in \mathcal{P}}} \mu^2(d)|R_d| = O_u\left(\frac{X}{\log^{\kappa+u} X} \right)$$

mit $\kappa = 2$ und $\alpha = 1 - \epsilon$ erfüllt sind.
Aus Lemma 3.7.1 folgt die Existenz einer Konstanten λ mit $0 < \lambda^{1+\lambda} < 1$ mit

$$1 - \frac{2\lambda^2 e^{2\lambda}}{1 - \lambda^2 e^{2+2\lambda}} > 0 \quad \text{und} \quad 1 + \frac{2,01}{e^\lambda - 1} < 8.$$

Mit $z = n^{\zeta_0}$, $u = \frac{\log X}{\log z} = 8 + o(1)$ für $n \to \infty$ und der Wahl $b = 1$ folgt dann $S(\mathcal{A}, \mathcal{P}, n^{\zeta_0}) \to \infty$ für genügend kleines ϵ und $n \to \infty$.
Es gibt also $h_0 \in \mathcal{A}$ mit $q(h_0) \geq n^{\zeta_0}$ und $q(h_0 2^{l_0} - 1) \geq n^{\zeta_0}$. Wir setzen $k_0 = h_0 2^{l_0} - 1$.
Es gilt dann

$$p|k_0 \Rightarrow p \geq n^{\zeta_0} \quad \text{bzw.} \quad p|\frac{k_0 + 1}{2^{l_0}} \Rightarrow p \geq n^{\zeta_0}. \tag{7}$$

Wir kommen nun zum

- 2. Schritt:
  Es sei $\mathcal{B} = \{w \cdot \frac{n-w}{d_0} : 1 \leq w \leq \frac{1}{4}n^{1-9\zeta_0},\ w \equiv n \bmod k_0\}$. Es gibt dann n_0 mit $0 \leq n_0 < k_0$, so dass für $w \in \mathcal{B}$ die Aussage $w \equiv n_0 \bmod k_0$ gilt, also $w = s \cdot k_0 + n_0$ mit $1 \leq s \cdot k_0 + n_0 \leq \frac{1}{4}n^{1-9\zeta_0}$.
  Damit haben wir

$$\mathcal{B} = \left\{ (sk_0 + n_0) \cdot \left(\frac{n - n_0}{k_0} - s \right) : sk_0 + n_0 \leq \frac{1}{4}n^{1-9\zeta_0} \right\}.$$

  Wir wenden Satz 3.7.1 mit

$$X = k_0^{-1} \cdot \left(\frac{1}{4}n^{1-9\zeta_0} - n_0 \right) \tag{8}$$

  an. Wir definieren $\omega(p)$ als die Anzahl der Lösungen der Kongruenz

$$(sk_0 + n_0) \cdot \left(\frac{n - n_0}{k_0} - s_0 \right) \equiv 0 \bmod p. \tag{9}$$

Jede der beiden Kongruenzen

$$sk_0 + n_0 \equiv 0 \bmod p \quad \text{und} \quad \frac{n - n_0}{k_0} - s_0 \equiv 0 \bmod p$$

hat höchstens eine Lösung modulo p. Also gilt $\omega(p) \leq 2$.
Für die aus $\omega(p)$ durch Multiplikativität erhaltene Funktion $\omega(d)$ gilt

$$\omega(d) \leq 2^{\nu(d)}. \tag{10}$$

Jedes Intervall der Länge d enthält $\omega(d)$ Lösungen von

$$(sk_0 + n_0) \cdot \left(\frac{n - n_0}{k_0} - s \right) \equiv 0 \bmod d,$$

die aus den Lösungen von (8) mittels des Chinesischen Restsatzes genommen werden können.
Aufteilen des Intervalls $(0, X]$ in Teilintervalle der Länge d zeigt, dass $|\mathcal{B}_d| = \frac{\omega(d)}{d} X + R_d$ mit $|R_d| \leq 2^{\nu(d)}$ gilt.
Wiederum sind (R_0) mit $L = 1$ und $A_0' = 2$ sowie $(R_1(\kappa, \alpha))$ mit $\kappa = 2$ und $\alpha = 1 - \epsilon$ erfüllt.
Wir setzen

$$z = 3n^{9\zeta_0}. \tag{11}$$

Wegen $n^{\zeta_0} \leq 2^{l_0} < 2n^{\zeta_0}$, $\frac{1}{2} n^{8\zeta_0} < h_0 \leq n^{8\zeta_0}$ und $k_0 = h_0 2^{l_0} - 1$ folgt $\frac{1}{3} n^{9\zeta_0} < k_0 \leq 2n^{9\zeta_0}$. Weiter folgt wegen $X = k_0^{-1} \left(\frac{1}{4} n^{1-9\zeta_0} - n_0 \right)$

$$X \geq n^{4/5}. \tag{12}$$

Aus (11) und (12) folgt

$$u = \frac{\log X}{\log z} \geq 8.$$

Nach Satz 3.7.1 folgt $S(\mathcal{B}, \mathcal{P}, z) \to \infty$ für $n \to \infty$.
Es gibt also ein w mit $w \leq \frac{1}{4} n^{1-9\zeta_0}$ und $m = \frac{n-w}{k_0} \in \mathbb{N}$. bzw.

$$q(w) \geq 3n^{9\zeta_0}. \tag{13}$$

Es ist

$$m \geq \frac{n}{k_0} - 1 \geq \frac{1}{2} n^{1-9\zeta_0} - 1 > w \geq 1 \tag{14}$$

und

$$q^+(m) \geq k_0. \tag{15}$$

Damit gilt nach Satz 2.1.2 (Satz von Mac Neish)

$$N(m) \geq k_0 - 1. \tag{16}$$

Nach (13) bis (16) sind die Bedingungen von Satz 2.3.4 erfüllt, und wir erhalten

$$N(km + w) \geq \min\{N(m), N(w), N(k_0) - 1, N(k_0 + 1) - 1\}.$$

Nach Satz 2.1.2 ist

$$N(w) \geq n^{\zeta_0}. \tag{17}$$

Nach Satz 2.1.2, wegen (7), (16), (17) und wegen $2^{l_0} \geq n^{\zeta_0}$ folgt für $n \geq n_0$

$$N(n) \geq n^{\zeta_0} - 1 \geq n^{1/91}.$$

Damit ist die Behauptung von Satz 3.8.1 für den Fall 1 bewiesen.

Im Unterschied zu Fall 1 setzen wir bei Fall 2 im 1. Schritt $\mathcal{A} = \{h(2^{l_0} h + 1) \colon \frac{1}{2} n^{8\zeta_0} < h \leq n^{8\zeta_0}\}$ und wählen $k_0 = h_0 \cdot 2^{l_0}$.

□

Kapitel 4

Nichtexistenz von projektiven Ebenen

4.1 Die Inzidenzmatrix eines Designs

Definition 4.1.1. Ein Design $D(v, b, r, k, \lambda)$ habe die Objekte $a_1, \ldots, a_v$ und die Blöcke $\mathcal{B}_1, \ldots, \mathcal{B}_b$. Die Inzidenzmatrix von D ist die Matrix $A = (a_{ij})_{\substack{1 \le i \le v \\ 1 \le j \le b}}$ mit

$$a_{ij} = \begin{cases} 1 & \text{für } a_i \in \mathcal{B}_i \\ 0 & \text{für } a_i \notin \mathcal{B}_i. \end{cases}$$

Es bedeute w_m den Zeilenvektor, der aus m Einsen besteht, und es bedeute $\mathcal{E}_m$ die Einheitsmatrix vom Typ $m \times m$ und $\mathcal{J}_m$ die Matrix vom Typ $m \times m$ mit Einsen als Einträgen:

$$\mathcal{J}_m = \begin{pmatrix} 1 & \ldots & 1 \\ \vdots & & \vdots \\ 1 & \ldots & 1 \end{pmatrix}.$$

Satz 4.1.1. *Für die Inzidenzmatrix A eines Designs $D(v, b, r, k, \lambda)$ gilt*

$$A \cdot A^T = \begin{pmatrix} r & \lambda & \ldots & \lambda \\ \lambda & \ddots & & \vdots \\ \vdots & & \ddots & \vdots \\ \lambda & \ldots & \lambda & r \end{pmatrix} = (r - \lambda)\mathcal{E}_v + \lambda \mathcal{J}_v.$$

Beweis. Wir schreiben $A \cdot A^T = (b_{ij})_{1 \le i,j \le v}$. Dann ist b_{ij} das innere Produkt der i- ten und j- ten Zeilen von A. Für $i \neq j$ ist b_{ij} die Anzahl der gemeinsamen Einsen in der i- ten und j- ten Zeile, also nach Definition 4.1.1 gleich λ, der Anzahl der Blöcke, in denen a_i und a_j gemeinsam auftreten.
Für $i = j$ ist b_{ii} die Anzahl der Einsen in der i- ten Zeile, also gleich r, der Anzahl der Blöcke, in denen a_i vorkommt.
Daraus ergibt sich die Behauptung. □

Definition 4.1.2. Ein Design $D(v, b, r, k, \lambda)$ heißt symmetrisch, falls $v = b$ gilt.

Satz 4.1.2. *In einem symmetrischen Design gilt $r = k$.*

Beweis. Dies folgt aus der Gleichung $b \cdot k = v \cdot r$ von Satz 1.2.1 und aus Definition 4.1.2. □

Beispiel 4.1.1. Nach Satz 1.4.2 ist eine projektive Ebene der Ordnung n ein Design mit den Parametern $D(n^2+n+1, n^2+n+1, n+1, n+1, 1)$, also ein symmetrisches Design.

Satz 4.1.3. *Es sei $(\mathcal{D}, \mathcal{B})$ ein symmetrisches Design $D(v, v, r, r, \lambda)$ mit $v \geq 2$.*
Dann ist $r > \lambda$. Die Inzidenzmatrix A von D ist quadratisch vom Typ $v \times v$ und nicht singulär.
Ist v gerade, so ist $r - \lambda$ eine Quadratzahl.

Beweis. Es ist klar, dass $\lambda \leq r$ gilt.

Annahme: $\lambda = r$

Dann liegt jedes Paar von verschiedenen Objekten a_i und a_j gemeinsam in $\lambda = r$ Blöcken.
Da auch a_i und a_j einzeln in r Blöcken liegen, enthält jeder Block sämtliche Objekte.
Nach Definition 1.2.1 sind die Blöcke verschiedene Teilmengen von $\mathcal{D}$. Also ist $v = r = \lambda = 1$, ein Widerspruch zu $v \geq 2$.
Nach Definition 4.1.1 ist A vom Typ $v \times v$.
Nach Satz 4.1.1 ist

$$A \cdot A^T = \begin{pmatrix} r & \lambda & \dots & \lambda \\ \lambda & \ddots & & \vdots \\ \vdots & & \ddots & \vdots \\ \lambda & \dots & \lambda & r \end{pmatrix}.$$

Wir berechnen die Determinante $\det(A \cdot A^T)$. In einem ersten Schritt subtrahieren wir die erste Spalte von allen anderen und erhalten die Matrix

$$\begin{pmatrix} r & \lambda - r & \dots & & \lambda - r \\ \lambda & r - \lambda & 0 & \dots & 0 \\ \lambda & 0 & r - \lambda & 0 & 0 \\ \vdots & \vdots & \dots & \ddots & \\ \lambda & 0 & \dots & 0 & r - \lambda \end{pmatrix}$$

In einem zweiten Schritt addieren wir die zweite bis v- te Zeile zur ersten und erhalten die untere Dreiecksmatrix

$$\begin{pmatrix} r + (v-1) \cdot \lambda & 0 & \dots & 0 \\ & r - \lambda & 0 & \vdots \\ * & & \ddots & \vdots \\ & & & r - \lambda \end{pmatrix}$$

mit Determinante $(r - \lambda)^{v-1} \cdot (v\lambda - \lambda + r)$. Also gilt

$$\det(A \cdot A^T) = (\det A)^2 = (r - \lambda)^{v-1} \cdot (v\lambda - \lambda + r) \neq 0. \tag{1}$$

Damit ist A nicht singulär.
Aus der Gleichung $r \cdot (k-1) = \lambda \cdot (v-1)$ von Satz 1.2.1 ergibt sich $k \cdot (k-1) = \lambda \cdot (v-1)$, woraus sich

$$\lambda v - \lambda + r = k^2$$

äergibt. Wegen (1) ist auch $(r - \lambda)^{v-1}$ eine Quadratzahl, und da $v - 1$ ungerade ist, auch $r - \lambda$. $\square$

4.2 Designs und Äquivalenz von quadratischen Formen

Im folgenden sei stets K ein Körper mit $1 + 1 \neq 0$.

Definition 4.2.1. Es sei $n \in \mathbb{N}$. Unter $K^{(n,n)}$ verstehen wir die Menge aller Matrizen $\mathcal{A} = (a_{ij})_{1 \leq i,j \leq n}$ vom Typ $n \times n$ mit $a_{ij} \in K$.
Die Matrix $\mathcal{A}$ heißt symmetrisch, falls $a_{ij} = a_{ji}$ für alle $1 \leq i, j \leq n$ gilt. Die Menge aller invertierbaren Matrizen von $K^{(n,n)}$ wird $GL(n, K)$ genannt.
Es sei $\vec{e}_i = (0, 0, \ldots, 0, 1, 0, \ldots, 0)$, wobei die 1 an der i- ten Stelle steht.

Definition 4.2.2. Es sei $n \in \mathbb{N}$. Unter einer Bilinearform B auf K^n versteht man eine Abbildung $B\colon K^n \times K^n \to K$, $(\vec{x}, \vec{y})$, die in beiden Argumenten linear ist, d.h.

$$\begin{aligned} B(\lambda_1\vec{x}_1 + \lambda_2\vec{x}_2, \vec{y}) &= \lambda_1 B(\vec{x}_1, \vec{y}) + \lambda_2 B(\vec{x}_2, \vec{y}) \\ B(\vec{x}, \mu_1\vec{y}_1 + \mu_2\vec{y}_2) &= \mu_1 B(\vec{x}, \vec{y}_1) + \mu_2 B(\vec{x}, \vec{y}_2) \end{aligned}$$

für alle $\vec{x}_i, \vec{y}_i, \vec{x}, \vec{y} \in K^n$ und $\lambda_i, \mu_i \in K$.
Die Abbildung B heißt symmetrisch, falls $B(\vec{x}, \vec{y}) = B)\vec{y}, \vec{x})$ für alle $\vec{x}, \vec{y} \in K^n$ gilt.

Satz 4.2.1. *Es sei $n \in \mathbb{N}$, B eine Bilinearform auf K und $\mathcal{A} = (a_{ij}) \in K^{(n,n)}$.*
Es gilt genau dann $B(\vec{x}, \vec{y}) = \vec{x}^T\mathcal{A}\vec{y}$ für alle $\vec{x}, \vec{y} \in K^n$, wenn $a_{ij} = B(\vec{e}_i, \vec{e}_j)$ gilt.
Insbesondere ist $\mathcal{A}$ durch B eindeutig bestimmt. Weiter ist B genau dann symmetrisch, wenn $\mathcal{A}$ symmetrisch ist.

Beweis. Durch Nachrechnen. □

Definition 4.2.3. Es sei $n \in \mathbb{N}$ und $\mathcal{A} \in K^{(n,n)}$ symmetrisch.
Dann versteht man unter der quadratischen Form Q mit der Matrix $\mathcal{A}$ die Abbildung

$$Q\colon K^n \to K, \vec{x} \to Q(\vec{x}) = \vec{x}^T\mathcal{A}\vec{x}. \tag{1}$$

Satz 4.2.2. *Die symmetrische Matrix $\mathcal{A}$ in (1) ist durch Q eindeutig bestimmt.*

Beweis. Wie man leicht nachrechnet, ist die durch $Q(\vec{x} + \vec{y}) = Q(\vec{x}) + 2B(\vec{x}, \vec{y}) + Q(\vec{y})$ definierte Abbildung $B\colon K^n \times K^n \to K$ eine symmetrische Bilinearform mit Matrix $\mathcal{A}$. Durch Q ist B eindeutig bestimmt. Nach Satz 4.2.1 ist $\mathcal{A}$ durch B eindeutig bestimmt und daher auch durch Q. □

Definition 4.2.4. Es sei $Q\colon K^n \to K$ eine quadratische Form. Die nach Satz 4.2.2 eindeutig bestimmte symmetrische Matrix $\mathcal{A}$ mit (1) bezeichnen wir mit $M(Q)$.

Definition 4.2.5. Es sei $n \in \mathbb{N}$ und Q_1, Q_2 quadratische Formen über K mit $M(Q_1) = \mathcal{A}_1 \in K^{(n,n)}$ bzw. $M(Q_2) = \mathcal{A}_2 \in K^{(n,n)}$. Wir nennen Q_1 und Q_2 äquivalent (über K), falls es ein $\mathcal{C} \in GL(n, K)$ mit $\mathcal{A}_2 = \mathcal{C}^T\mathcal{A}_1\mathcal{C}$ gibt.

Satz 4.2.3. *Es sei $n \in \mathbb{N}$.*

i) Die Äquivalenz von quadratischen Formen ist eine Äquivalenzrelation auf der Menge aller quadratischer Formen Q mit $M(Q) \in K^{(n,n)}$.

ii) Äquivalente quadratische Formen stellen dieselben Elemente aus $K^{(n,n)}$ dar.

Beweis. i) Symmetrie:

$$\mathcal{A}_2 = \mathcal{C}^T \mathcal{A}_1 \mathcal{C} \Rightarrow \mathcal{A}_1 = (\mathcal{C}^{-1})^T \mathcal{A}_2 \mathcal{C}^{-1}$$

Transitivität:
Es sei $\mathcal{A}_2 = \mathcal{C}^T \mathcal{A}_1 \mathcal{C}$ und $\mathcal{A}_3 = \mathcal{D}^T \mathcal{A}_2 \mathcal{D}$. Dann gilt $\mathcal{A}_3 = (\mathcal{C}\mathcal{D})^T \mathcal{A}_1 \mathcal{C}\mathcal{D}$.
Reflexivität:
Es gilt $\mathcal{A} = \mathcal{E}_n^T \mathcal{A} \mathcal{E}_n$ mit der Einheitsmatrix $\mathcal{E}_n \in K^{(n,n)}$.

ii) Es sei $M(Q_1) = \mathcal{A}_1$, $M(Q_2) = \mathcal{A}_2$ und $\mathcal{A}_2 = \mathcal{C}^T \mathcal{A}_1 \mathcal{C}$. Dann gilt

$$Q_2(\mathcal{C}^{-1}\vec{x}) = \vec{x}^T (\mathcal{C}^{-1})^T \mathcal{A}_2 \mathcal{C}^{-1} \vec{x} = \vec{x}^T (\mathcal{C}^{-1})^T \mathcal{C}^T \mathcal{A}_1 \mathcal{C}\mathcal{C}^{-1} \vec{x} = \vec{x}^T \mathcal{A}_1 \vec{x} = Q_1(\vec{x}).$$

□

Definition 4.2.6. Eine quadratische Form Q heißt nicht ausgeartet, falls $M(Q)$ nicht singulär ist, ansonsten ausgeartet.

Satz 4.2.4. *Aus der Existenz eines symmetrischen Designs $D(v, v, r, r, \lambda)$ mit $v \geq 2$ folgt die Äquivalenz über dem Körper $\mathbb{Q}$ der rationalen Zahlen von folgenden quadratischen Formen: $Q_1, Q_2 \colon \mathbb{Q}^v \to \mathbb{Q}$ mit $Q_1(\vec{x}) = (r-\lambda) \cdot (x_1^2 + \ldots + x_v^2) + \lambda \cdot (x_1 + \ldots + x_v)^2$ und $Q_2(\vec{x}) = x_1^2 + \ldots + x_v^2$.*

Beweis. Es sei A die Inzidenzmatrix des Designs. Nach Satz 4.1.1 ist

$$A \cdot A^T = A^T \cdot A = (r-\lambda) \cdot \mathcal{E}_v + \lambda \cdot \mathcal{J}_v = M(Q_1).$$

Wegen $M(Q_2) = \mathcal{E}_v$ folgt damit $M(Q_1) = A^T M(Q_2) A$, wobei A nach Satz 4.1.3 nichtsingulär ist.
Das Ergebnis folgt nach Definition 4.2.4. □

4.3 p- adische Körper

Die Äquivalenz von quadratischen Formen über dem Körper $\mathbb{Q}$ der rationalen Zahlen impliziert auch deren Äquivalenz über dem Körper $\mathbb{R}$ der reellen Zahlen. Die Umkehrung gilt nicht. Jedoch können weitere Körper, die Körper $\mathbb{Q}_p$ der p- adischen Zahlen für jede Primzahl p eingeführt werden, so dass gilt:
Zwei quadratische Formen Q_1 und Q_2 über $\mathbb{Q}$ sind genau dann über $\mathbb{Q}$ äquivalent, wenn sie über $\mathbb{R}$ und für jede Primzahl p über $\mathbb{Q}_p$ äquivalent sind.

In diesem Abschnitt geben wir eine Einführung in die Theorie der p- adischen Zahlen.
Eine mögliche Weise, die reellen Zahlen aus den rationalen Zahlen zu konstruieren, ist, sie als Cauchyfolgen zu definieren.

Definition 4.3.1. Eine rationale Cauchyfolge ist eine Folge $(a_n)_{n\in\mathbb{N}}$ mit $a_n \in \mathbb{Q}$, für die gilt:

$$\forall \epsilon > 0 \; \exists n_0 = n_0(\epsilon) \colon \forall m, n \geq n_0 \colon |a_m - a_n| < \epsilon.$$

Dieser Definition liegt der gewöhnliche Absolutbetrag zugrunde.

Definition 4.3.2. Zwei Cauchyfolgen (a_n) und (b_n) heißen äquivalent (Schreibweise: $(a_n) \sim (b_n)$), wenn ihre Differenz eine Nullfolge bildet.
Unter einer Nullfolge versteht man eine Folge (c_n), für die gilt:

$$\forall \epsilon > 0 \; \exists n_0 = n_0(\epsilon) \colon \forall n \geq n_0 \colon |c_n| < \epsilon.$$

Unter der Menge $\mathbb{R}$ aller reeller Zahlen versteht man die Menge der Äquivalenzklassen $(\overline{a_n})$ aller rationaler Cauchyfolgen.

Man kann die rationalen Zahlen $\mathbb{Q}$ in $\mathbb{R}$ "einbetten", indem man die Äquivalenzklassen konstanter Folgen $(r, r, \ldots, r, \ldots)$ mit $r \in \mathbb{Q}$ identifiziert. Die Verknüpfungen der Addition und der Multiplikation lassen sich von den rationalen Zahlen mittels der Grenzwertsätze auf $\mathbb{R}$ übertragen.

Definition 4.3.3. Es ist

$$\begin{aligned}(\overline{a_n}) + (\overline{b_n}) &= (\overline{a_n + b_n}) \\ (\overline{a_n}) \cdot (\overline{b_n}) &= (\overline{a_n \cdot b_n}).\end{aligned}$$

Satz 4.3.1. *Das Nullelement von $\mathbb{R}$ ist die Äquivalenzklasse der Nullfolgen.*
Gilt $(\overline{a_n}) \neq 0$, so ist a_n^{-1} eine rationale Cauchyfolge, und es ist $(\overline{a_n}) \cdot (\overline{a_n^{-1}}) = 1$.
Durch Definition 4.3.3 sind Addition und Multiplikation wohldefiniert. Weiter ist $\mathbb{R}$ vollständig und ein Körper. Jede Cauchyfolge reeller Zahlen konvergiert.

Für eine Primzahl p erhält man nun der Körper $\mathbb{Q}_p$ der p- adischen Zahlen, indem man dieses Verfahren zur Konstruktion der reellen Zahlen kopiert, mit der einzigen Änderung, dass der gewöhnliche Absolutbetrag, der in Definition 4.3.1 zur Definition der Cauchyfolge verwendet wurde, nun durch den p- adischen Betrag (auch p- Betrag) ersetzt wird.

Definition 4.3.4. Es sei $r \in \mathbb{Q}$ und $r \neq 0$. Dann hat r eine eindeutige Darstellung der Form

$$r = \frac{a}{b} \cdot p^n$$

mit $a, b, n \in \mathbb{Z}$ und $(a, b) = (a, p) = (b, p) = 1$. Der Exponent $n := \nu_p(r)$ heißt die p- Bewertung von r. Man setzt $\nu_p(0) = \infty$. Dann heißt

$$|r|_p := \begin{cases} p^{-\nu_p(r)} & \text{für } r \neq 0 \\ 0 & \text{für } r = 0 \end{cases}$$

der p- Betrag von r.

Lemma 4.3.1. *Für $x, y \in \mathbb{Q}$ gilt*

i) $\nu_p(xy) = \nu_p(x) + \nu_p(y)$ sowie $\nu_p(x + y) \geq \min\{\nu_p(x), \nu_p(y)\}$

ii) Ist $\nu_p(x) \neq \nu_p(y)$, so gilt $\nu_p(x + y) = \min\{\nu_p(x), \nu_p(y)\}$.

Beweis. i) klar!

ii) Es sei $x = \frac{a}{b}p^m$ und $y = \frac{c}{d}p^n$ mit $m \geq n$. Dann ist für $p \nmid abcd$

$$x + y = p^n \cdot \left(\frac{a}{b}p^{m-n} + \frac{c}{d}\right) = p^n \cdot \frac{adp^{m-n} + cb}{bd},$$

also gilt $\nu_p(x + y) \geq \nu_p(y)$ mit $p \nmid bd$.
Ist $m > n$, so folgt $p \nmid (adp^{m-n} + cb)$ und damit $\nu_p(x + y) = \nu_p(y)$.

□

Lemma 4.3.2. *Für $x, y \in \mathbb{Q}$ gilt*

$$\begin{aligned}|xy|_p &= |x|_p \cdot |y|_p \\ |x + y|_p &\leq \max\{|x|_p.|y|_p\}.\end{aligned}$$

Ist $|x|_p \neq |y|_p$, so gilt sogar $|x + y|_p = \max\{|x|_p, |y|_p\}$.

Definition 4.3.5. Es seien $x, y \in \mathbb{Q}$. Die Zahl $d_p(x,y) = |x-y|_p$ heißt der p- adische Abstand von x und y.

Beispiel 4.3.1. Es gilt

$$\begin{aligned} d_2(3,51) &= \frac{1}{16} \\ d_3(3,51) &= \frac{1}{3} \\ d_p(3,51) &= 1 \end{aligned}$$

für $p \notin \{2,3\}$.

Satz 4.3.2. *Es sei p eine Primzahl. Dann ist der p- adische Abstand d_p eine Metrik auf $\mathbb{Q}$, d.h. es gilt*

i) $d_p(x,y) = d_p(y,x)$ *für alle* $x, y \in \mathbb{Q}$ *(Symmetrie)*

ii) $d_p(x,z) \leq d_p(x,y) + d_p(y,z)$ *für alle* $x, y, z \in \mathbb{Q}$ *(Dreiecksungleichung)*

iii) $d_p(x,y) \geq 0$ *und* $d_p(x,y) = 0$ *genau dann, wenn* $x = y$ *ist (positive Definitheit).*

Es gilt sogar die verschärfte Dreiecksungleichung: $d_p(x,z) \leq \max\{d_p(x,y), d_p(y,z)\}$.

Definition 4.3.6. Es sei p eine Primzahl. Unter einer p- adischen Cauchyfolge versteht man eine Folge (a_n) rationaler Zahlen, für die gilt:

$$\forall \epsilon > 0 \; \exists n_0 = n_0(\epsilon) \colon \forall m, n \geq n_0 \colon d_p(a_m, a_n) = |a_m - a_n|_p < \epsilon.$$

Weiter heißt (a_n) eine p- adische Nullfolge, falls

$$\forall \epsilon > 0 \; \exists n_0 = n_0(\epsilon) \colon \forall n \geq n_0 \colon |a_n|_p < \epsilon.$$

Zwei p- adische Cauchyfolgen (a_n) und (b_n) heißen äquivalent (Schreibweise: $(a_n) \sim (b_n)$), falls $(a_n - b_n)$ eine p- adische Nullfolge bildet.
Unter der Menge $\mathbb{Q}_p$ der p- adischen Zahlen versteht man die Menge aller Äquivalenzklassen (a_n) von p- adischen Cauchyfolgen (a_n). Die Menge $\mathbb{Q}$ der rationalen Zahlen kann in $\mathbb{Q}_p$ eingebettet werden, indem man die Äquivalenzklasse der konstanten Folge $(r, r, \ldots, r)$ mit $r \in \mathbb{Q}$ identifiziert.

Ähnlich wie in Definition 4.3.3 für die reellen Zahlen können wir nun auch auf $\mathbb{Q}_p$ die Verknüpfung Addition und Multiplikation sowie die multiplikativen Inversen definieren.

Definition 4.3.7. Es seien (a_n) und (b_n) zwei p- adische Cauchyfolgen. Dann setzen wir

$$\begin{aligned} (\overline{a_n}) + (\overline{b_n}) &= (\overline{a_n + b_n}) \\ (\overline{a_n}) \cdot (\overline{b_n}) &= (\overline{a_n \cdot b_n}). \end{aligned}$$

Satz 4.3.3. *Durch Definition 4.3.7 sind Addition und Multiplikation auf $\mathbb{Q}_p$ wohldefiniert. Das Nullelement von $\mathbb{Q}_p$ ist die Äquivalenzklasse der Nullfolgen.*
Gilt $(\overline{a_n}) \neq 0$*, so ist* a_n^{-1} *eine p- adische Cauchyfolge, und es ist* $(\overline{a_n}) \cdot (\overline{a_n^{-1}}) = 1$.
Somit ist $\mathbb{Q}_p$ ein Körper. Außerdem ist Q_p vollständig, d.h. jede Folge von p- adischen Cauchyfolgen p- adischer Zahlen konvergiert.

Beispiel 4.3.2. Zeige, dass die Gleichung $x^2 = -1$ eine Lösung in $\mathbb{Q}_5$ hat.

Lösung:
Wir finden rekursiv Lösuungen x_m von

$$x_m^2 \equiv -1 \bmod 5^m \qquad (C_m)$$

für alle m.

$\underline{m=1}$:
Es ist $x_1 = 2$ eine Lösung von (C_1).

$\underline{m=2}$:
Setze $x_2 = x_1 + 5u_1$ mit $0 \leq u_1 \leq 4$. Dann wird (C_2) zu

$$\begin{aligned} & x_1^2 + 10x_1u_1 + 5^2u_1^2 \equiv -1 \bmod 5^2 \\ \Leftrightarrow \quad & 4 + 20u_1 + 5^2u_1^2 \equiv -1 \bmod 5^2 \\ \Leftrightarrow \quad & 1 + 4u_1 \equiv 0 \bmod 5^2 \\ \Leftrightarrow \quad & u_1 \equiv 1 \bmod 5 \end{aligned}$$

und damit $x_2 = 2 + 1 \cdot 5$, denn u_1 ist durch die Forderung $0 \leq u_1 \leq 4$ eindeutig bestimmt.

$\underline{m \to m+1}$:
Es sei $x_m = x_1 + 5u_1 + \ldots + u_{m-1}5^{m-1}$ eine Lösung von $x_m^2 \equiv -1 \bmod 5^m$.
Wir setzen $x_{m+1} = x_m + 5^m u_m$ mit $0 \leq u_m \leq 4$. Dann wird (C_{m+1}) zu

$$\begin{aligned} & x_{m+1}^2 = x_m^2 + 2 \cdot 5^m u_m + 5^{2m}u_m^2 \equiv -1 \bmod 5^{m+1} \\ \Leftrightarrow \quad & x_m^2 + 1 + 2 \cdot 5^m \equiv 0 \bmod 5^{m+1} \\ \Leftrightarrow \quad & \frac{x_m^2 + 1}{5^m} + 2u_m \equiv 0 \bmod 5, \end{aligned}$$

und die letzte Kongruenz hat eine eindeutig bestimmte Lösung modulo 5 mit $0 \leq u_m \leq 4$.
Damit hat (C_{m+1}) eine eindeutig bestimmte Lösung $x_{m+1} = x_1 + 5u_1 + \ldots + u_m 5^m$ mit $0 \leq u_j \leq 4$.
Die Folge (x_m) bildet eine 5- adische Cauchyfolge: Es sei $m_1 < m_2$. Dann gilt

$$d_p(x_{m_1}, x_{m_2}) = |u_{m_1+1}5^{m_1+1} + \ldots + u_{m_2}5^{m_2}|_5 = |u_{m_1+1}5^{m_1+1}|_5 = 5^{-(m_1+1)}.$$

Damit ist die Äquivalenzklasse der Cauchyfolge (x_m) ein Element von $\mathbb{Q}_5$. Man hat die Darstellung als unendliche Reihe, die in $\mathbb{Q}_5$, aber nicht in $\mathbb{R}$ konvergiert, als

$$x = u_0 + 5u_1 + \ldots u_m 5^m + \ldots = \sum_{m=0}^{\infty} u_m 5^m$$

mit $u_0 = 2$.
Auch (x_m^2) bildet eine 5- adische Cauchyfolge. Es ist

$$\lim_{m \to \infty} |x_m^2 - (-1)|_5 = 0.$$

Damit ist (x_m^2) zur Folge $(-1, -1, \ldots, -1, \ldots)$ äquivalent, also $x^2 = -1$.

Wir verallgemeinern das Ergebnis von Beispiel 4.3.2 zu

Satz 4.3.4. *(Henselsches Lemma)*
Es sei p eine Primzahl und f ein Polynom mit ganzzahligen Koeffizienten.
Dann lässt sich jede Lösung $x = \tilde{x_l}$ von $f(x) \equiv 0 \bmod p$, für die $f'(\tilde{x_l}) \not\equiv 0 \bmod p$ ist, eindeutig zu einer Lösung von $f(x_l) = 0$ mit $x_l \in \mathbb{Q}_p$ fortsetzen. Dabei hat x_l eine eindeutig bestimmte Reihenentwicklung

$$x_l = u_0^{(l)} + u_1^{(l)}p + \ldots + u_m^{(l)}p^m$$

mit $0 \leq u_i^{(l)} \leq p-1$. Es ist $u_0^{(l)} = \tilde{x_l}$.

Beweis. (Skizze)
Es sei $\tilde{x}_l$ eine Lösung von $f(x) \equiv 0 \bmod p$. Um dies zu einer Lösung von

$$f(x) \equiv 0 \bmod p^2 \tag{C_2}$$

fortzusetzen, setzen wir

$$x_2^{(l)} = u_0^{(l)} + u_1^{(l)} \cdot p$$

mit $u_0^{(l)} = \tilde{x}_l$. Wir haben die Taylorentwicklung

$$\begin{aligned} f(x_2^{(l)}) &= f(u_0^{(l)} + u_1^{(l)} \cdot p) = f(u_0^{(l)}) + f'(u_1^{(l)}) \cdot u_1^{(l)} \cdot p + \frac{f''(u_0^{(l)}}{2!} \cdot (u_1^{(l)})^2 \cdot p^2 + \ldots \\ &\equiv f(u_0^{(l)}) + f'(u_0^{(l)} \cdot u_1^{(l)} \cdot p \bmod p^2. \end{aligned}$$

Wegen $f(u_0^{(l)}) \neq 0 \bmod p$ wird (C_2) zu

$$\frac{f(u_0^{(l)})}{p} + f'(u_0^{(l)}) \cdot u_1^{(l)} \bmod p,$$

was wegen $f'(u_0^{(l)}) \neq 0 \bmod p$ eine modulo p eindeutig bestimmte Lösung $u_1^{(l)} \bmod p$ hat. Durch die Forderung $0 \leq u_1^{(l)} \leq p-1$ ist $u_1^{(l)}$ eindeutig bestimmt.
$m \to m+1$:
Es sei $x_m^{(l)} = u_0^{(l)} + u_1^{(l)} \cdot p + \ldots + u_{m-1}^{(l)} \cdot p^{m-1}$ eine Lösung von $f(x_m^{(l)}) \equiv 0 \bmod p^m$.
Wir setzen $x_{m+1} = x_m^{(l)} + u_m^{(l)} \cdot p^m$. Die Kongruenz $f(x_{m+1}^{(l)}) \equiv 0 \bmod p^{m+1}$ wird dann zu

$$f(x_{m+1}^{(l)}) = f(x_m^{(l)}) + u_m \cdot f'(x_m^{(l)}) \cdot p^m + r_m \bmod p^{m+1}$$

mit $r_m \equiv 0 \bmod p^{2m}$. Wegen $f(x_m^{(l)}) \equiv 0 \bmod p^m$ wird dies zu

$$\frac{f(x_m^{(l)})}{p^m} + u_m \cdot f'(x_m^{(l)}) \equiv 0 \bmod p,$$

was wiederum wegen $f'(x_{,}^{(l)}) \equiv f'(\tilde{x}_l) \neq 0 \bmod p$ eine eindeutige Lösung u_m mit $0 \leq u_m \leq p-1$ hat. Durch die unendliche Reihe

$$x_l = \sum_{m=0}^{\infty} u_m^{(l)} p^m \in \mathbb{Q}_p$$

ist eine Lösung von $f(x) = 0$ gegeben. □

4.4 Der Satz von Hasse-Minkowski

Satz 4.4.1. *(Hasse- Minkowski)*
Zwei rationale quadratische Formen Q_1 und Q_2 sind genau dann äquivalent, wenn sie über $\mathbb{R}$ und für jede Primzahl p über $\mathbb{Q}_p$ äquivalent sind.

Wir benötigen also Kriterien für die Äquivalenz über $\mathbb{R}$ und über $\mathbb{Q}_p$.
Kriterien für die Äquivalenz über $\mathbb{R}$ beruhen auf dem Trägheitssatz von Sylvester.

Satz 4.4.2. *(Sylvesterscher Trägheitssatz)*
Es seien $r, r', s, s' \in \mathbb{N}_0$ *sowie*

$$\begin{aligned} Q_{(r,s)} &= x_1^2 + \ldots + x_r^2 - x_{r+1}^2 - \ldots - x_{r+s}^2 \\ Q_{(r',s')} &= x_1^2 + \ldots + x_{r'}^2 - x_{r'+1}^2 - \ldots - x_{r'+s'}^2. \end{aligned}$$

Dann sind $Q_{(r,s)}$ *und* $Q_{(r'.s')}$ *genau dann über* $\mathbb{R}$ *äquivalent, wenn* $(r, s) = (r', s')$ *gilt.*

Satz 4.4.3. *Eine nichtausgeartete quadratische Form über* $\mathbb{R}$ *ist zu* $Q_{(r,s)}$ *für genau ein Paar* $(r, s) \in \mathbb{N}_0^2$ *äquivalent.*

Definition 4.4.1. Unter der Signatur (r, s) einer nichtausgearteten quadratischen Form Q über $\mathbb{R}$ versteht man das nach Satz 4.4.2 eindeutig bestimmte Paar (r, s), so dass $Q \sim Q_{(r,s)}$ gilt.
Man nennt Q positiv definit, wenn $r = n$ gilt, negativ definit, wenn $s = n$ ist und indefinit, wenn $rs \neq 0$ ist.

Aus Satz 4.4.2 und Satz 4.4.3 folgt nun

Satz 4.4.4. *Zwei quadratische Formen sind genau dann über* $\mathbb{R}$ *äquivalent, wenn sie dieselbe Signatur haben.*

Zur Überprüfung der Äquivalenz von quadratischen Formen über $\mathbb{Q}_p$ benötigen wir die Begriffe des Hilbertsymbols und der Hasseinvariante.

Definition 4.4.2. Es sei p eine Primzahl und $a, b \in \mathbb{Q}_p \backslash \{0\}$. das Hilbertsymbol $(a, b)_p$ ist durch $(a, b)_p = 1$ definiert, sofern die Gleichung $ax^2 + by^2 = z^2$ eine Lösung in $\mathbb{Q}_p^3$ mit $(x, y, z) \neq (0, 0, 0)$ besitzt. Andernfalls sei $(a, b)_p = -1$.
Es sei Q eine nichtausgeartete quadratische Form vom Rang n über $\mathbb{Q}_p$, und es sei $Q \sim \tilde{Q}$ mit $\tilde{Q}(x_1, \ldots, x_n) = a_1 x_1^2 + \ldots + a_n x_n^2$. Dann ist die Hasseinvariante $\epsilon_p(Q)$ durch

$$\epsilon_p(Q) = \prod_{1 \leq i < j \leq n} (a_i, a_j)_p$$

gegeben.

Satz 4.4.5. *Es sei* $n \in \mathbb{N}$, p *eine Primzahl sowie* Q_1 *und* Q_2 *quadratische Formen über* $\mathbb{Q}_p$ *in* n *variablen. Dann sind* Q_1 *und* Q_2 *genau dann äquivalent über* $\mathbb{Q}_p$, *wenn* $\epsilon(Q_1) = \epsilon(Q_2)$ *gilt.*

Die Berechnung von Hassesymbolen lässt sich nach Definition 4.4.2 auf die Berechnung von Hilbertsymbolen zurückführen. Die Berechnung von Hilbertsymbolen folgt aus den im folgenden Satz zusammengefassten Eigenschaften.

Satz 4.4.6. *Es sei p eine Primzahl und $b, c, d, e \in \mathbb{Z}$. Dann gilt*

i) $(b, c)_p = (c, b)_p$

ii) $(b_1 b_2, c)_p = (b_1, c)_p \cdot (b_2, c)_p$

iii) $(bd^2, ce^2)_p = (b, c)_p$

iv) $(b, -b)_p = -1$

v) $(b^2, c) = 1$

Falls p eine ungerade Primzahl ist, folgt

vi) $(b, c)_p = 1$, *falls* $p \nmid bc$

vii) $(b, c)_p = \left(\frac{b}{p}\right)$, *falls* $b \not\equiv 0 \bmod p$

viii) $(p, p)_p = (-1, p)_p$

Falls $b_1 \equiv b_2 \not\equiv 0 \bmod p$, so folgt $(b_1, c)_p = (b_2, c)_p$.

Es ist nun möglich, den Satz von Bruck, Chowla und Ryser auf den Satz von Hasse- Minkowski zurückzuführen. Wir werden jedoch im nächsten Abschnitt einen davon unabhängigen Beweis geben.

4.5 Der Satz von Bruck- Chowla- Ryser

Satz 4.5.1. *(Satz von Bruck- Chowla- Ryser)*
Es sei $(\mathcal{D}, \mathcal{B})$ ein symmetrisches Design $D(v, v, r, r, \lambda)$ mit $r \geq 3$ ungerade. Dann hat die Gleichung

$$z^2 = (r - \lambda) \cdot x^2 + (-1)^{\frac{v-1}{2}} \lambda \cdot y^2$$

eine Lösung in ganzen Zahlen x, y und z.

Beweis. Wir setzen $n := r - \lambda$.
Nach Satz 4.2.3 folgt aus der Existenz von $(\mathcal{D}, \mathcal{B})$ die Äquivalenz der quadratischen Formen

$$Q_1(\vec{x}) = n \cdot (x_1^2 + \ldots + x_v^2) + \lambda \cdot (x_1^2 + \ldots + x_v^2)$$

und $Q_2(\vec{x}) = x_1^2 + \ldots + x_v^2$ über dem Körper $\mathbb{Q}$ der rationalen Zahlen. Nach Definition 4.2.4 bedeutet dies die Existenz von $a_{ij} \in \mathbb{Q}$, so dass

$$L_1^2 + \ldots + L_v^2 = n \cdot (x_1^2 + \ldots + x_v^2) + \lambda \cdot (x_1^2 + \ldots + x_v^2) \tag{1}$$

für

$$L_j = \sum_{i=1}^{v} a_{ij} x_i.$$

Nach dem Vier- Quadrate- Satz von Lagrange gibt es $b_1, b_2, b_3, b_4 \in \mathbb{Z}$ mit $n = b_1^2 + b_2^2 + b_3^2 + b_4^2$.

Wir benutzen nun eine Identität, die bei gewisen Beweisen des Vier- Quadrate- Satzes ebenfalls eine Schlüsselrolle spielt. Es sei

$$\begin{aligned} y_1 &= b_1x_1 - b_2x_2 - b_3x_3 - b_4x_4 \\ y_2 &= b_2x_1 + b_1x_2 - b_4x_3 + b_3x_4 \\ y_3 &= b_3x_1 + b_4x_2 + b_1x_3 - b_2x_4 \\ y_4 &= b_4x_1 - b_3x_2 + b_2x_3 + b_1x_4 \end{aligned} \tag{2}$$

bzw.

$$\vec{y} = \mathcal{B}\vec{x} \quad \text{mit} \quad \mathcal{B} = \begin{pmatrix} b_1 & -b_2 & -b_3 & -b_4 \\ \vdots & & \vdots & \\ b_4 & \dots & & \end{pmatrix}.$$

Es ist $\mathcal{B}^T\mathcal{B} = n \cdot E_4$ und damit $\det \mathcal{B} = n^2$. Dann ist

$$(b_1^2 + b_2^2 + b_3^2 + b_4^2) \cdot (x_1^2 + x_2^2 + x_3^2 + x_4^2) = y_1^2 + y_2^2 + y_3^2 + y_4^2. \tag{3}$$

Diese Identität folgt in natürlicher Weise mittels des Schiefkörpers

$$\mathbb{H} = \{a_1 + a_2i + a_3j + a_4k \colon a_l \in \mathbb{R},\ 1 \le l \le 4\}$$

der Hamiltonschen Quaternionen. Es ist

$$(b_1 + b_2i + b_3j + b_4k) \cdot (x_1 + x_2i + x_3j + x_4k) = y_1 + y_2i + y_3j + y_4k.$$

Wenn wir die Norm $N(\beta)$ mit $\beta = b_1 + b_2i + b_3j + b_4k$ durch $N(\beta) = b_1^2 + b_2^2 + b_3^2 + b_4^2$ definieren, dann folgt (3) aus $N(\beta) \cdot N(\xi) = N(\beta\xi)$. Wir unterscheiden folgende Fälle:

- $v \equiv 1 \bmod 4$:
  Indem wir (2) und (3) mit den Indizes i, $i+1$, $i+2$ und $i+3$ anstelle von 1,2,3 und 4 benutzen, erhalten wir
  $$n \cdot (x_i^2 + x_{i+1}^2 + x_{i+2}^2 + x_{i+3}^2) = y_i^2 + y_{i+1}^2 + y_{i+2}^2 + y_{i+3}^2. \tag{4}$$
  Indem wir die Variablen in Blöcke von je vier einteilen und (4) anwenden, erhalten wir
  $$L_1^2 + \ldots + L_v^2 = y_1^2 + y_2^2 + \ldots + y_{v-1}^2 + nx_v^2 + \lambda \cdot (x_1 + \ldots + x_v)^2. \tag{5}$$
  Wegen $\det \mathcal{B} \neq 0$ kann (2) nach
  $$\begin{pmatrix} y_i \\ y_{i+1} \\ y_{i+2} \\ y_{i+3} \end{pmatrix} = \mathcal{B} \cdot \begin{pmatrix} x_i \\ x_{i+1} \\ x_{i+2} \\ x_{i+3} \end{pmatrix}$$
  zu
  $$\begin{pmatrix} x_i \\ x_{i+1} \\ x_{i+2} \\ x_{i+3} \end{pmatrix} = \mathcal{B}^{-1} \cdot \begin{pmatrix} y_i \\ y_{i+1} \\ y_{i+2} \\ y_{i+3} \end{pmatrix}$$
  aufgelöst werden, und wir erhalten
  $$L_j = \sum_{i=1}^{v} c_{ij} y_i \tag{6}$$
  mit $c_{ij} \in \mathbb{Q}$ sowie
  $$w = x_1 + \ldots + x_v = \sum_{i=1}^{v} \alpha_i y_i. \tag{7}$$

Aus (5) erhalten wir

$$L_1^2 + L_2^2 + \ldots + L_v^2 = y_1^2 + \ldots + y_{v-1}^2 + ny_v^2 + \lambda w^2,$$

wobei L_j und w durch (6) und (7) gegeben sind.
Es sei OBdA $c_{11} \neq 0$. Dann gibt es eine Linearkombination $\ell(y_2, \ldots, y_v)$ mit

$$L_1(\ell(y_2, \ldots, y_v), y_2, \ldots, y_v) = y_1.$$

Indem wir $\tilde{L}_j^{(2)}(y_2, \ldots, y_v) = L_j^{(2)}(\ell(y_2, \ldots, y_v), y_2, \ldots, y_v)$ und

$$\tilde{w}(y_2, \ldots, y_v) = w(\ell(y_2, \ldots, y_v), y_2, \ldots, y_v)$$

setzen, erhalten wir

$$\left(\tilde{L}_2^{(2)}\right)^2 + \ldots + \left(\tilde{L}_v^{(2)}\right)^2 = y_2^2 + \ldots + y_{v-1}^2 + ny_v^2 + \lambda\tilde{w}^2.$$

Wiederholung dieses Reduktionsprozesses führt zu

$$\left(\tilde{L}_v^{(2)}\right)^2 = ny_v^2 + \lambda\tilde{w}^2.$$

Wir wählen nun y_v als ein gemeinsames Vielfaches der Nenner, die in den Koeffizienten von $L_v^{(v)}$ auftreten und erhalten mit $x = y_v$, $z = L_v^{(v)}(y_v)$ und $y = w^{(v)}(y_v)$

$$nx^2 + \lambda y^2 = z^2. \tag{8}$$

- $v \equiv 3 \bmod 4$:
  Wir führen eine zusätzliche Variable x_{v+1} ein, addieren auf beiden Seiten des Ausdruckes (1) den Term nx_{v+1}^2 und erhalten durch Substitution von der Form (2)

  $$L_1^2 + L_2^2 + \ldots + L_v^2 + nx_{v+1}^2 = y_1^2 + \ldots + y_{v+1}^2 + \lambda w^2.$$

  Indem wir wie in Fall $v \equiv 1 \bmod 4$ vorgehen, erhalten wir

  $$nx^2 = y_{v+1}^2 + \lambda w^2$$

  und schließlich

  $$z^2 = nx^2 - \lambda y^2. \tag{9}$$

  Dann können (8) und (9) zu einer Gleichung zusammengefasst werden:

  $$z^2 = nx^2 + (-1)^{\frac{v-1}{2}}\lambda y^2,$$

  was den Beweis von Satz 4.5.1 beendet.

□

Satz 4.5.2. *Es sei $n \equiv 1 \bmod 4$ oder $n \equiv 2 \bmod 4$. Ist n nicht die Summe von zwei Quadratzahlen, so existiert keine projektive Ebene der Ordnung n.*

Beweis. Wir nehmen an, es existiere ine projektive Ebene der Ordnung n.
Es ist $v = n^2 + n + 1 \equiv 3 \bmod 4$ und $r = n + 1$. damit ist $\frac{v-1}{2} \equiv 1 \bmod 2$. Nach Satz 4.5.1 folgt

$$nx^2 = z^2 + y^2.$$

Aus der Elementaren Zahlentheorie ist bekannt, dass n^2 genau dann eine Summe von zwei Quadratzahlen ist, wenn jede in n in ungerader Potenz aufgehende Primzahl p entweder $p = 2$ oder $p \equiv 1 \bmod 4$ ist. Dies ist für n genau dann erfüllt, wenn es für nx^2 erfüllt ist. □

Abschließende Bemerkungen:

Es ist bisher keine projektive Ebene bekannt, deren Ordnung keine Primzahlpotenz ist.
Satz 4.5.2 liefert die Nichtexistenz von projektiven Ebenen für die Ordnungen

$$n \in \{6, 14, 21, 22, 30, 33, 38, 42, 46, \ldots\}.$$

Der einzige Fall, für den Satz 4.5.2 keine Antwort liefern konnte, ist der Fall $n = 10$. Unter Benutzung tiefer Beziehungen zur Codierungstheorie und mit massivem Computereinsatz konnte Lam 1984 die Nichtexistenz einer projektiven Ebene der Ordnung 10 zeigen.
Der kleinste unentschiedene Fall ist $n = 12$.
Für alle $n \in \mathbb{N}$, für die keine projektive Ebene der Ordnung n existiert, gilt $N(n) \leq n - 2$.
Dieses Ergebnis konnte leicht verbessert werden:
Es gebe keine projektive Ebene der Ordnung n. Weiter sei $p(x) = \frac{1}{2}x^4 + x^3 + x^2 + \frac{3}{2}x$, und d sei die größte Zahl, für die $p(d-1) < n$ gilt. Dann ist $N(n) \leq n - d - 2$ (Bruck, 1963).
Das Ergebnis $N(n) \geq n^{1/91}$ für $n \geq 10$ von Chowla- Erdös- Strauß konnte zu $N(n) \geq n^{1/14,8}$ verbessert werden.
Es ist nicht bekannt, ob es eine unendliche Folge von Nichtprimzahlpotenzen mit $N(n) \geq \sqrt{n}$ gibt.