Elementare Zahlentheorie

gehört bei Prof. Dr. Gekeler SS 2003

30. Juli 2003

Das Manuskript wurde erstellt von Herrn Christian Schmaltz und, was die Formulierung von Definitionen, Sätzen und Beweisen betrifft, von Prof. Gekeler autorisiert. Allerdings gibt es den Verlauf der Vorlesung nicht vollständig wieder, da zahlreiche Beispiele, Erinnerungen und mündliche Zwischenbemerkungen nicht aufgenommen wurden.

1 Teilbarkeit in $\mathbb{Z}$, Primzahlen

Definitionen 1.1 (Grundlegende Definitionen): Eine **Gruppe** ist eine Menge G mit einer Verknüpfung (Multiplikation)

$$G \times G \to G, \quad (x,y) \mapsto x \cdot y = xy$$

mit

1. $\exists\, 1_G = 1 \in G$ mit $1 \cdot x = x \cdot 1 = x \quad \forall x \in G$
2. $\forall x,y,z \in G$ ist $(xy)z = x(yz)$
3. $\forall x \in G\ \exists\, y \in G$ mit $xy = yx = 1$

y heißt die **Inverse** x^{-1} von x. Es gilt:

$$x^2 = x \cdot x, \quad x^3 = x \cdot x \cdot x, \quad x^n = x \cdot \ldots \cdot x \quad n \in \mathbb{N} \quad x^0 := 1, \quad x^{-n} = \underbrace{x^{-1}x^{-1} \cdots x^{-1}}_{n-Faktoren}$$

Eine Gruppe $(G,\cdot)$ heißt **kommutativ** oder **abelsch**, falls zusätzlich gilt:

$$xy = yx \quad \forall\, x,y \in G$$

Abelsche Gruppen werden meist **additiv** geschrieben:

$$G \times G \to G \quad (x,y) \mapsto x+y,$$

Neutralelement: $0_G = 0$ Inverse: $-x$ $\underbrace{x+x+\ldots+x}_{n-\text{ Summanden}}$ = nx (n $\in \mathbb{Z}$) Ist G eine nicht kommutative Gruppe, so gilt i.a. nicht

$$(xy)^n = x^n y^n, \text{ aber } \quad x^{n+m} = (x^n)(x^m) \text{ gilt immer.}$$

Ein **Ring** R ist eine Menge mit zwei Verknüpfungen "+", "·" mit

1. $(R,+)$ ist abelsche Gruppe
2. $\exists$ Neutralelement $1_R = 1$ bzgl. "$\cdot$" $1 \neq 0$
3. "·" ist assoziativ
4. $\forall\, x,y,z \in R$ gelte $x(y+z) = xy+xy$ und $(y+z)x = yx+zx$

R heißt **kommutativ**, falls zusätzlich gilt:

$$\forall\, x,y \in R \text{ ist } xy = yx$$

Ein **Körper** ist ein Ring $(K,+,\cdot)$, für den gilt:

1. $K\backslash\{0\}$ ist bgzl. "$\cdot$" eine kommutative Gruppe.

Äquivalent zu 1. sind $1'$ und $1''$:

$1'$: $\forall\, 0 \neq x \in K \quad \exists\, y \in K$ mit $xy = 1$.

$1''$ $\forall\, a,b \in K, a \neq 0$ hat $ax = b$ eine wohlbestimmte Lösung x in K.

Sind G und H multiplikative Gruppen, so ist ein **Homomorphismus** $\varphi : G \mapsto H$ eine Abbildung mit

1. $\varphi(xy) = \varphi(x)\varphi(y) \quad \forall x,y \in G$
2. $\varphi(1_G) = 1_H$

Sind R, S Ringe, so ist ein **(Ring-)Homomorphismus** von R nach S eine Abbildung $\varphi : R \to S$ mit

1. $\varphi(x+y) = \varphi(x) + \varphi(y)$
2. $\varphi(0_R) = 0_S$
3. $\varphi(xy) = \varphi(x)\varphi(y)$
4. $\varphi(1_R) = 1_S$

Eine **Untergruppe** der Gruppe $(G,\cdot)$ ist eine Teilmenge H von G mit

1. $H \neq \emptyset$
2. $\forall\, x,y \in H$ ist $xy^{-1} \in H$

Ein **Unterring** $(S,+,\cdot)$ des Rings $(R,+,\cdot)$ ist eine Teilmenge S mit

1. $(S,+)$ ist Untergruppe von $(R,+)$
2. $\forall\, x,y \in S$ ist $xy \in S$
3. $1_R \in S$

Ein **Ideal** von $(R,+,\cdot)$ ist eine Teilmenge $\mathfrak{I}$ von R mit

1. $(\mathfrak{I},+)$ ist Untergruppe von $(R,+)$
2. $\forall\, x \in R$, $\forall\, y \in \mathfrak{I}$ sind xy und $yx \in \mathfrak{I}$

Beachte: Unterring $\not\Rightarrow$ Ideal und Ideal $\not\Rightarrow$ Unterring.

Ist G eine Gruppe, $H_i (i \in I)$ seien Untergruppen. Dann ist $\bigcap\{H_i | i \in I\}$ wieder eine Untergruppe von G. Entsprechendes gilt für "Unterringe" bzw. "Ideale" eines Rings R. Sei jetzt R ein kommutativer Ring und $A \subset R$ eine Teilmenge.

$$\langle A\rangle := \{x \in R \mid \exists \text{ endlich viele } a_1,\ldots,a_n \in A, r_1,\ldots,r_n \in R \text{ mit } x = r_1a_1 + r_2a_2 + \ldots r_na_n\}$$

ist ein Ideal von R, und zwar das kleinste Ideal von R, das A umfaßt. $\langle A\rangle$ heißt das von A erzeugte Ideal.

Ein Ideal der Form

$$R_a = \langle\{a\}\rangle = \{ra | r \in R\}, a \in R$$

heißt **Hauptideal**.

Zahlenbereiche 1.2 ($\mathbb{N},\mathbb{Z},\mathbb{C}\ldots$):

- $\mathbb{N}=\{1,2,3,\ldots\},\mathbb{N}_0=\{0,1,2,3,\ldots\},\mathbb{Z},\mathbb{Q}\,\mathbb{R},\mathbb{C}=\{a+bi|a,b\in\mathbb{R},\ i^2=-1\}$
- Auf $\mathbb{C}$ (und damit auf $\mathbb{R}$) existiert der **Absolutbetrag**: $|a+bi|:=\sqrt{a^2+b^2}$.
  Er erfüllt $|x+y|\leq|x|+|y|$ ($\triangle$-Ungleichung).
- $\mathbb{R}$ und $\mathbb{C}$ sind Cauchy-vollständig.
- Ist $\emptyset\neq S\subset\mathbb{N}$, so existiert min($S$) = x in S, d.h. $\forall\, y\in S$ ist $x\leq y$.
- Ist $\emptyset\neq S\subset\mathbb{N}$ beschränkt, so $\exists$ max(S).
- Ist $S\subset\mathbb{N}$ mit

  1. $1\in S$
  2. $n\in S\Rightarrow n+1\in S$

  so ist $S=\mathbb{N}$ (vollst. Induktion)

Definition 1.3 (Teilbarkeit, prim, zusammengesetzt):

- Seien $a,\ b\in\mathbb{Z}$. b teilt $a:\Leftrightarrow\exists\, c\in\mathbb{Z}:a=bc$ Schreibweise: $b|\ a$, “b Teiler von a”
- a ist **Primzahl** oder prim $:\Leftrightarrow\{a,b>1;(b|\ a)\Rightarrow(b=a)\}$
- a heißt **zusammengesetzt** $:\Leftrightarrow a\in\mathbb{N}\backslash\{1\},a$ nicht prim.
- Setze $\mathbb{P}:=\{2,3,5,7,11,\ldots\}$ für die Menge der Primzahlen.
- Beachte: $\mathbb{N}=\mathbb{P}\dot{\cup}\{1\}\dot{\cup}\{a\in\mathbb{N}|a$ zusammengesetzt$\}$.

Satz 1.4 (Primfaktorzerlegung): Jedes $k\in\mathbb{N}$ ist Produkt von Primzahlen.

Beweis : $n=1$ und $n=2$ sind klar. Für $n>2$ ist n entweder prim oder $n=ab$, $a,b>1$ und $a,b<n$.

Nach Induktionsvoraussetzung sind a,b Produkte von Primzahlen, also auch $n=ab$.

□

Definition 1.5 (ggT): $a,b\in\mathbb{Z}\,(a,b)\neq(0,0)$. Setze $(a,b):=ggT(a,b):=\max\{n\in\mathbb{Z}|n|\ a\wedge n|\ b\}$.

a und b heißen **teilerfremd** (**relativ prim**, **koprim**), falls $(a,b)=1$.

Satz 1.6 (Euklid): Sind $f,g\in\mathbb{Z},f\geq 0,g>0$. Dann $\exists!\ q,r\geq 0$ mit $(f=gq+r)\wedge(r<q)$

Beweis : Eindeutigkeit: Seien $f=gq+r=g'q+r'$ zwei derartige Paare $(g,r),(g',r')$.

O.B.d.A gelte $r\leq r'$. Dann ist $(g-g')q=r'-r$.

Wäre $g-g'\neq 0$, so $q\leq|(g-g')q|\leq r'<q$. Widerspruch.

Deshalb gilt $g=g'$ und $r=r'$.

Existenz: (Induktion nach f) $\quad f<q:g=0,r=f$

Ist $f\geq q$, so folgt: $f-g=g'q+r\Rightarrow f=\underbrace{(g'+1)}_{g}q+r$.

□

Satz 1.7 (Ideale in $\mathbb{Z}$): Jedes Ideal des Ringes $\mathbb{Z}$ ist ein Hauptideal.

Beweis : Sei $\mathfrak{I} \subset \mathbb{Z}$ ein Ideal. $\mathfrak{I} = \{0\} = \mathbb{Z} \cdot 0$ ist Hauptideal.

Ist $\mathfrak{I} \neq \{0\}$, so sei $q \in \mathfrak{I}, q > 0$, minimal mit diesen Eigenschaften.

Beh.: $\mathfrak{I} = \mathbb{Z}q$.

Ist nämlich $f \in \mathfrak{I}$, o.B.d.A $f \geq 0$, so $\exists!$ (g,r) wie in 1.6 mit $f = gq + r$

Es ist $r \in \mathfrak{I}$ und $\quad 0 \leq r < q$.

Nach Konstruktion ist also $r = 0$, und deshalb $f = gq$. Damit ist die Behauptung gezeigt, und damit der Satz.

□

Satz 1.8 (Summe von Idealen in $\mathbb{Z}$): Seien $a, b \in \mathbb{Z}$, nicht beide 0. Dann ist

$$\mathbb{Z}a + \mathbb{Z}b = \langle \{a,b\} \rangle = \langle ggT(a,b) \rangle = \mathbb{Z}ggT(a,b)$$

Beweis : Nach 1.7 ist $\mathbb{Z}a + \mathbb{Z}b = \mathbb{Z}c$ für ein $c \in \mathbb{Z}, c \geq 0$. Wegen $a \in \mathbb{Z}c$ gilt $c \mid a$, ebenso $c \mid b$. Also $c \leq g$ nach Definition von $g = (a,b)$. Andererseits folgt aus $g \mid a$ und $g \mid b$:

$g \mid ax + by \quad \forall\, x,y \in \mathbb{Z} \rightarrow g \mid c$.

Zusammen folgt $c = g$.

□

Korollar 1.9 (Lineare Gleichungen): Die Gleichung $ax + by = n$ ($a,b,n \in \mathbb{Z}$ gegeben) hat genau dann ganzzahlige Lösungen (x,y), falls $(a,b) \mid n$.

□

Satz 1.10 (Euklid): Seien $a, b \in \mathbb{Z}$ teilerfremd. Für $c \in \mathbb{Z}$ gilt:

$$a \mid bc \Rightarrow a \mid c$$

Beweis : $(a,b) = 1 \rightsquigarrow \exists\, x,y \in \mathbb{Z}$ mit $ax + by = 1 \rightsquigarrow c = (ax + by)c = acx + bcy$ teilbar durch a

□

Korollar 1.11 (Satz von Euklid): Sei $p \in \mathbb{P}, a, b \in \mathbb{Z}$.

Aus $p \mid ab \wedge p \nmid a$ folgt, daß $p \mid b$ gilt.

□

Korollar 1.12 (Satz von Euklid): Seien $p, p_1, \ldots, p_s$ Primzahlen. Aus $p \mid (p_1 p_2 \ldots p_s)$ folgt: $\exists i$ mit $p = p_i$.

□

Korollar 1.13 (Satz von Euklid): Seien $a, b \in \mathbb{Z}, (a,b) = 1$ Dann gilt für $x \in \mathbb{Z}$:

$$(x, ab) = 1 \Leftrightarrow (x,a) = (x,b) = 1$$

□

Definition 1.14 (Standardform): Eine **Standardform** für $n \in \mathbb{N}$ ist eine Produktdarstellung

$$n = \prod_{1 \leq i \leq r} p_i^{e_i}, \quad p_1 < p_2 < \ldots < p_r \text{ Primzahlen }, e_i \in \mathbb{N}.$$

Satz 1.15 (Eindeutige Primfaktorzerlegung): Jedes $n \in \mathbb{N}$ besitzt genau eine Standardform.

Beweis : Die Existenz einer Standardform ist Satz 1.4.

Eindeutigkeit: Seien $n = \prod_{1\le i\le r} p_i^{e_i} = \prod_{1\le j\le s} q_i^{e_i}$ zwei Standardformen.

Wegen (1.12) folgt: $\{p_i\} = \{q_j\}$, wobei $r = s$.

Annahme: $e_i \neq e_i'$ für ein i. Dann ist $\frac{n}{p_i^{e_i}} \in \mathbb{N},\ e_i < e_i'$

$$\underbrace{\frac{n}{p_i^{e_i}}}_{\text{Kein Faktor } p_i} = \prod_{1\le j\le r, j\neq i} p_j^{e_j'} \underbrace{p_i^{e_i'-e_i}}_{\text{mindestens ein Faktor } p_i}$$. Widerspruch.

Satz 1.16 (Euklid): Es gilt unendlich viele Primzahlen.

Beweis : Sei $\emptyset \neq S \subset \mathbb{P}$, $\#(S) < \infty$. Wir zeigen: Es existiert eine Primzahl $p \notin S$.

Sei $N(S) := \prod_{q\in S} q + 1$ und sei p ein Primteiler von $N(S)$. Dann ist $p \notin S$, denn jedes $q \in S$ hat die Eigenschaft:

$N(S)$ läßt beim Teilen durch q den Rest 1.

□

Probleme 1.17 (Primzahlschranken): Sei p_i die i-te Primzahl, $(p_1 = 2, p_2 = 3, p_3 = 5, \ldots)$

- Finde eine Formel für p_i, d.h. eine berechenbare Funktion

  $$f : \mathbb{N} \to \mathbb{P} \quad \text{mit } f(i) = p_i \quad \text{(Zu schwierig!)}$$

  Beispiel: Es gibt eine reelle Zahl Θ, die die Information über alle Primzahlen kodiert.
- Finde Schranken f_1, f_2, so daß für alle (vielleicht: für alle genügend großen) i gilt:

  $$f_1(i) \le p_i \le f_2(i)$$

  Setze $\Pi(x) := \#\{p \in \mathbb{P} | p \le x\}, x \in \mathbb{P}$.
- Finde Schranken g_1, g_2 mit $g_1(x) \le \Pi(x) \le g_2(x)$.

Satz 1.18 (Schranke für Primzahlen): Für alle $n \in \mathbb{N}$ gilt $p_n \le 2^{2^{n-1}}$.

Beweis : Per Induktion nach n. $n = 1 : p_1 = 2$

$n > 1$: $N := 1 + \prod_{1\le i\le n-1} p_i$. Nach dem Beweis von 1.16 gibt es ein $m \ge n$ mit $p_m | N$. Dann gilt:

$p_n \le p_m \le 1 + \prod_{1\le i\le n-1} p_i \le 1 + 2^{2^0} 2^{2^1} \cdots 2^{2^{n-2}} = 1 + 2^{2^{n-1}-1} \le 2^{2^n}$.

□

Beispiel (Schranke für Primzahlen): $n = 10, \quad p_{10} = 29 : \quad 2^{2^{n-1}} = 2^{512} \approx 1{,}34 \cdot 10^{154}$

Also ist die durch (1.18) gegebene Schranke sehr schlecht!

Definition 1.19 (Fermat-Zahlen): Für $n \in \mathbb{N}_0$ sei $F_n := 2^{2^n} + 1$ die n-te Fermat-Zahl.

$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65537$

Fermat hat behauptet: Alle F_n sind Primzahlen. Dies ist richtig für $n \le 4$.

Satz 1.20 (Teilerfremdheit der Fermat-Zahlen): Alle F_n sind teilerfremd.

Beweis : 1. Wir zeigen durch Induktion: $\prod_{0\le i\le n-1} F_i = F_n - 2$

Der Fall $n = 1$ ist klar. Für $n \to n+1$ gilt:

$$\prod_{0\le i\le n} F_i = F_n \prod_{0\le i\le n-1} F_i \overset{I.V.}{=} (2^{2^n}+1)(2^{2^n}-1) = (2^{2^{n+1}}-1) = F_{n+1} - 2$$

2. Sei nun t ein Teiler von F_i und F_n, $i < n$.

Wegen 1. ist $t = 1$ oder $t = 2$. Da alle F_n ungerade sind, ist $t = 1$.

□

2 Kongruenzrechnung

Definition 2.1 (modulo): Sei $n \in \mathbb{N}$. Definiere auf $\mathbb{Z}$ die Relation

$$a \equiv b \pmod{n} :\Leftrightarrow n \mid (a-b)$$

"Kongruenz modulo n", in Zeichen $a \equiv b \pmod{n}$ oder $a \equiv b(n)$.

Lemma/Definition 2.2 ($\mathbb{Z}/n\mathbb{Z}$): "Kongruenz modulo n" ist eine Äquivalenzrelation. Schreibe $\mathbb{Z}/n\mathbb{Z}$ oder $\mathbb{Z}/n$ für die Menge der Äquivalenzklassen bzgl. dieser Relation. Setze "$\overline{a}$", "$a+n\mathbb{Z}$" oder "a mod n" für die Klasse von $n \in \mathbb{Z}$.

Beweis : im Prinzip beweisbedürftig ...

□

Lemma 2.3 ($\mathbb{Z}/n$ als Ring.): Sei $n \in \mathbb{N}, n > 1$. Die folgenden Verknüpfungen "+", "·" definieren auf $\mathbb{Z}/n$ eine Struktur als kommutativer Ring:

$$\overline{a}+\overline{b} = \overline{a+b} \quad \overline{a}\cdot\overline{b} = \overline{(ab)} \quad a,b \in \mathbb{Z}$$

Die Restklassenabbildung

$$\mathbb{Z} \to \mathbb{Z}/n \quad a \mapsto \overline{a}$$

ist ein surjektiver Ringhomomorphismus mit Kern $n\mathbb{Z}$.

Beweis : Klar.

□

Definition (Einheit): Ist R ein Ring, so heißt $e \in R$ **Einheit**, falls $e' \in R$ existiert mit $ee' = e'e = 1$. In diesem Fall ist das Inverse $e' = e^{-1}$ eindeutig bestimmt. Die Menge aller Einheiten von R bildet eine Gruppe unter der Multiplikation und wird mit R^* bezeichnet.

Beispiel: $\mathbb{Z}^* = \{\pm 1\}$, $R = \mathrm{Mat}(n,K)$, K Körper, $R^* = GL(n,K)$.

Was ist $(\mathbb{Z}/n)^*$?

Satz 2.4 (Einheiten in $\mathbb{Z}/n$): Sei $a \in \mathbb{Z}$ mit Restklasse $\overline{a} \in \mathbb{Z}/n$ $(1 < n \in \mathbb{N})$. Dann gilt: $\overline{a}$ ist Einheit in $\mathbb{Z}/n \Leftrightarrow (a,n) = 1$.

Beweis : $(a,n) = 1 \rightsquigarrow \exists\, x,y \in \mathbb{Z}$ mit $ax + ny = 1 \rightsquigarrow ax \equiv 1$, d.h. $\overline{a}$ invertierbar.

Umgekehrt: $ax \equiv 1(n) \rightsquigarrow \exists\, y \in \mathbb{Z}$ mit $ax + ny = 1 \rightsquigarrow (a,n) = 1$.

Korollar 2.5 ($\mathbb{Z}/n$): Sei $n \in \mathbb{N}$. Es gilt $n \in \mathbb{P} \Leftrightarrow \mathbb{Z}/n$ ist Körper.

Beispiele 2.6 ($\mathbb{Z}/n\mathbb{Z}$):

1. $p = 11$ ist prim, also ist $\mathbb{Z}/11$ ein Körper. Deshalb existiert zu a mit $(a,11) = 1$ ein b mit $ab = ba \equiv 1 \pmod{11}$. Folgende Tabelle gibt diese Inversen an:

a	1	2	3	4	5	6	7	8	9	10
b	1	6	4	3	9	2	8	7	5	10

2. $n = 12$, $\quad (\mathbb{Z}/12)^* = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}\}$

Definition 2.7 (Eulersche φ-Funktion): Für $n \in \mathbb{N}$ sei definiert:

$$\varphi(n) := \begin{cases} \#(\mathbb{Z}/n)^* & n > 1 \\ 1 & n = 1 \end{cases}$$

$\varphi : \mathbb{N} \mapsto \mathbb{N}$ heißt die **Eulersche φ-Funktion**.

Satz 2.8 (Euler-Fermat): Ist $a \in \mathbb{Z}$ teilerfremd zu $n, 1 < n \in \mathbb{N}$, so gilt:

$$a^{\varphi(n)} \equiv 1 (\text{mod } n)$$

Insbesondere: Ist $n = p$ eine Primzahl, so ist $a^{p-1} \equiv 1 \pmod{p}$.

Beispiel: $2^{16} \equiv 1 \pmod{17}, \quad 7^4 \equiv 1 \pmod{12}$.

Beweis : Wir erinnern uns (?), daß für eine endliche Gruppe G und ein $x \in G$ gilt:

(*) $\text{ord}_G(x) \mid \#G \quad$ wobei $\quad \text{ord}_G(x) = \min\{i \in \mathbb{N} | x^i = 1\}$.

Es ist $\#((\mathbb{Z}/n)^*) = \varphi(n)$, also für $\varphi(n) = \text{ord}(\overline{a})t \quad (t \in \mathbb{N}, \overline{a} \in (\mathbb{Z}/n))$

$(\overline{a})^{\varphi(n)} = (\overline{a}^{\text{ord}(\overline{a})})^t = (\overline{1})^t = \overline{1}$.

also $a^{\varphi(n)} \equiv 1 \pmod{n}$, für alle $a \in \mathbb{N}$ mit $\text{ggT}(a,n) = 1$

□

Beweis von (*):

1. Sei $r := \text{ord}_G(x)$. Dann ist $\{x, x^2, x^3, \ldots, x^r = 1\} = \langle x \rangle$ eine Untergruppe von G.
2. $\#\langle x \rangle = r$
3. Ist $H \subset G$ eine Untergruppe, so definiert

   $$X \equiv y \pmod{H} :\Leftrightarrow xH = yH$$

   $$\Leftrightarrow \exists\, h \in H \text{ mit } xh = y \Leftrightarrow x^{-1}y \in H$$

   eine Äquivalenzrelation auf G.
4. Für jedes Paar (x,y) aus G ist

   $$xH \to yH \quad z \mapsto yx^{-1}z \quad (\text{bzw. } xh \mapsto yh)$$

   bijektiv.
5. Wegen

   $$G = \dot{\bigcup}_{\substack{x\text{laufe durch ein Repräsentantensystem} \\ \text{bzgl. der Äquivalenzrelation}}} xH$$

   folgt: $\#(G) = \#\{\text{Äquivalenzklassen}\} \cdot \#(H)$

□

Satz 2.9 ($\mathbb{Z}/nm$): Seien $m, n \in \mathbb{N}$ teilerfremd, beide > 1.

$A = \{a\}$ sei ein Repräsentantensystem für $\mathbb{Z}/m \quad (\#(A) = m)$

$B = \{b\}$ sei ein Repräsentantensystem für $\mathbb{Z}/n \quad (\#(B) = n)$

Es gelten:

1. $\{am + bn | \, a \in A, b \in B\}$ ist ein Repräsentantensystem für $\mathbb{Z}/mn$. Insbesondere sind alle $am + bn$ wie oben paarweise verschieden.
2. $am + bn$ ist invertierbar modulo $mn \Leftrightarrow$ { a invertierbar modulo n, b invertierbar modulo m }

Beweis :

1. Wir zeigen: die $\overline{am+bn}$ sind paarweise verschieden. Seien nämlich $am+bn \equiv a'm+b'n(n)(mn)$ mit $a,a' \in A, b,b' \in B \rightsquigarrow am+bn \equiv a'm+b'n(n) \rightsquigarrow am \equiv a'm(n)$. Da $(m,n)=1$ ist, existiert ein $m^* \in \mathbb{Z}$ mit $mm^* \equiv 1(n) \rightsquigarrow a \equiv m^*am \overset{(n)}{\equiv} m^*a'm \equiv a'$.
   Analog folgt: $b \equiv b' \pmod m$
2. $\overline{am+bn}$ invertierbar in $(\mathbb{Z}/mn)^* \Leftrightarrow (am+bn,mn)=1 \overset{1,13}{\Leftrightarrow} \left\{ \begin{array}{c} (am+bn,m)=1 \\ (am+bn,n)=1 \end{array} \right\} \Leftrightarrow \left\{ \begin{array}{c} (bn,m)=1 \\ (am,n)=1 \end{array} \right\}$

$$\overset{(m,n)=1}{\Leftrightarrow} \left\{ \begin{array}{c} (b,m)=1 \\ (a,n)=1 \end{array} \right\} \Leftrightarrow \left\{ \begin{array}{c} \overline{b} \in (\mathbb{Z}/m) \text{ invertierbar} \\ \overline{a} \in (\mathbb{Z}/n) \text{ invertierbar} \end{array} \right\}$$

□

Definition 2.10 (Schwach multiplikativ): Eine Abbildung $\alpha : \mathbb{N} \mapsto \mathbb{C}$ heißt **schwach multiplikativ**, falls gilt:

$$\alpha(mn) = \alpha(m)\alpha(n), \quad \text{falls ggT}(m,n) = 1.$$

Ist α schwach multiplikativ, und ist $n = \prod_{1 \le i \le r} p_i^{e_i}$ die Primfaktorzerlegung von $n \in \mathbb{N}$ (d.h. alle p_i sind verschieden), so gilt:

$$\alpha(n) = \prod_{1 \le i \le r} \alpha(p_i^{e_i})$$

Korollar 2.11 (φ und Multiplikativität): φ ist schwach multiplikativ.

Beweis : Seien m, n teilerfremd. Dann gilt:

$$\varphi(mn) = \#((\mathbb{Z}/mn)^*) = \#((\mathbb{Z}/m)^*)\#((\mathbb{Z}/n)) = \varphi(m)\varphi(n).$$

□

Korollar 2.12 (Formel für $\varphi(n)$): Sei $n = \prod_{1 \le i \le r} p_i^{e_i}$ die Primfaktorzerlegung von n. Dann ist

$$\varphi(n) = \prod_{1 \le i \le r} p_i^{e_i-1}(p_i-1).$$

Beweis : Es reicht zu zeigen: $\varphi(p^e) = p^{e-1}(p-1) \quad \forall\, p \in \mathbb{P}, e \in \mathbb{N}$.
Es ist $\varphi(p^e) = \#((\mathbb{Z}/p^e)^*) = \{a \in \mathbb{N} | 1 \le a \le p^e, (a,p^e)=1\} = p^e - p^{e-1} = p^{e-1}(p-1)$

□

Beispiel 2.13 ($\varphi(n)$): Sei $n = 2^2 3^2 5$. Dann ist $\varphi(180) = 2 \cdot (3 \cdot 2) \cdot 4 = 48$ Zusammen mit Euler-Fermat gilt dann:

$$a^{48} \equiv 1 \pmod{180}, \quad \text{falls (a,180) = 1, z.B. a = 7}$$

Naive Berechnung: $7^{48} \approx 3,67 \cdot 10^{40}$

Frage: Wie berechnet man z.B. $7^{48} \pmod{180}$ effizient?

Algorithmus 2.14 (Berechnung von $a^b \pmod c$): Seien $a \in \mathbb{R}, k \in \mathbb{N}$ gegeben. Ist

$$k = k_0 + k_1 \cdot 2 + k_2 \cdot 2^2 + \ldots + k_t \cdot 2^t, \quad k_t \in \{0,1\}$$

die Binärdarstellung von k (wobei $t = [log_2 k]$, d.h. der ganzzahlige Anteil von $log_2 k$), so kann man a^k mit der Formel

$$a^k = ((a^{k_t})^{2+k_{t_1}})^{2+kt_2} \ldots)^{2+k_0}$$

berechnen. Dabei werden höchstens $2t$ Operationen von Typ “Multiplikation” oder “Quadratur” benötigt, also nur logarithmisch viele.

Zur Berechnung von $a^b \pmod c$ sind außerdem folgende Schritte sinnvoll:

- Reduziere $\pmod n$ nach jedem Rechenschritt.
- Ist sogar $\varphi(n)$ bekannt, und ist $k_0 \equiv k \pmod{\varphi(n)}$, $(a,n)=1$, so ist $a^k \equiv a^{k_0} \pmod n$.

Satz 2.15 (Chinesischer Restsatz): Seien $m_1,\ldots,m_r$ paarweise teilerfremde natürliche Zahlen, die alle größer 1 sind und seien $a_1,\ldots,a_r \in \mathbb{Z}$ beliebig. Dann existiert $x \in \mathbb{Z}$ mit

$$x \equiv a_i \pmod{m_i} \quad i = 1,2,\ldots,r.$$

Dieses x ist bis auf Kongruenz modulo $n := \prod_{1\le i\le r} m_i$ eindeutig bestimmt.

Beweis : Existenz:

Setze $n_i = \frac{m}{m_i} \in \mathbb{N}$. Dann ist $(n_i, m_i) = 1$, und es existiert $n_i^* \in \mathbb{N}$ mit $n_i \cdot n_i^* \equiv 1 \pmod{m_i}$

Setze $x = a_1 n_1 n_1^* + a_2 n_2 n_2^* + \ldots + a_r n_r n_r^*$. Dieses x erfüllt die Kongruenzen, denn:

Für $j \neq i$ ist $n_i \mid n_j$, deshalb ist $x \equiv a_i n_i n_i^* \pmod{m_i}$, also $x \equiv a \pmod{m_i}$

Eindeutigkeit:

Seien $x,y \in \mathbb{Z}$ simultane Lösungen der Kongruenz $x \equiv a_i \equiv y \pmod{m_i} \quad \forall i$. Dann gilt:

$m_i \mid (x-y) \rightsquigarrow m \mid (x-y) \rightsquigarrow x \equiv y \pmod{m}$

□

Dieser Satz ist äquivalent zu:

Satz (Chinesischer Restsatz, 2. Variante): Sind $m_1,\ldots m_r$ alle größer eins und paarweise teilerfremd und $m := \prod_{1\le i\le r} m_i$, so ist die Abbildung

$$\mathbb{Z}/m \to \mathbb{Z}/m_1 \times \mathbb{Z}/m_2 \times \ldots \mathbb{Z}/m_r$$

$$a \pmod{m} \mapsto (a \pmod{m_1}, \ldots, a \pmod{m_r})$$

wohldefiniert und ein Isomorphismus von Ringen.

Beispiele 2.16 (Chinesischer Restsatz):

- $(m_1,m_2) = (2,3) \quad (a_1,a_2) = (1,2)$ Suche x mit $x \equiv 1(2), x \equiv 2(3)$, z.B. $x = 5$
- $(m_1,m_2) = (2^3,3^2) \quad (a_1,a_2) = (5,8)$. Hier ist $x = 53$ eine Lösung.

Problem 2.17 (Primzahlen und Restklassen): Gegeben sei $a \in \mathbb{Z}, 1 < n \in \mathbb{N}$. Gibt es (sogar unendlich viele) Primzahlen p mit $p \equiv a \pmod{n}$?

$$\begin{array}{lllll} \underline{Beispiel}: & n=4 & a=1 & p\equiv 1(4)? & Ja, z.B.\ 5,13,17,25\ldots \\ & & a=3 & p\equiv 3(4)? & Ja, z.B.\ 3,7,11,19\ldots \end{array}$$

Ist $(a,n) > 1$, so wird jedes $x \in \mathbb{Z}$ mit $x \equiv a \pmod{n}$ von (a,n) geteilt. Es kann also nur dann Primzahlen p mit $p \equiv a \pmod{n}$ geben, wenn $q := (a,m)$ Primzahl ist, und in diesem Fall ist $p = q$.

Satz (Dirichlet, hier ohne Beweis): Ist $(a,n) = 1, n > 1$, so existieren unendlich viele Primzahlen $p \in \mathbb{P}$ mit $p \equiv a \pmod{n}$.

Genauer:

$$\lim_{x\to\infty} \frac{\#\{p \in \mathbb{P} \mid p \equiv a \pmod{n}, p \le x\}}{\#\{p \in \mathbb{P} \mid p \le x\}} = \frac{1}{\varphi(n)}$$

Satz 2.18 (Primzahlen und Restklassen modulo 4): Es gibt unendlich viele $p \in \mathbb{P}$ mit $p \equiv 3 \pmod{4}$.

Beweis : Sei $S \subset \mathbb{P}, S$ endlich, $p \in S$ impliziere $p \equiv 3 \pmod{4}$.

Setze $N(S) := 4\prod_{p\in S} p - 1$

- Wir zeigen: $N(S)$ hat mindestens einen Primteiler $q \equiv 3(4)$: Da $N(S)$ ungerade ist, sind alle Primteiler von $N(S)$ kongruent zu 1 oder 3 $\pmod{4}$. Wären aber alle Primteiler kongruent zu 1(4), so würde dies auch für $N(S)$ gelten, denn das Produkt zweier Zahlen, die kongruent zu 1(4) sind, ist wieder kongruent zu 1(4).
- Sei q wie oben. Dann ist $q \notin S$, denn $q \in S$ würde $N(S) \equiv -1(q)$ implizieren.

□

Satz 2.19 (Nullstellen von Polynomen):

Sei $p \in \mathbb{P}, f(x) = \sum_{0 \le i \le n} a_i x^i, \quad a_i \in \mathbb{Z}$ ein Polynom mit $a_n \not\equiv 0 \pmod p$. Die Kongruenz $f(x) \equiv 0 \pmod p$ hat höchstens n Lösungen in $\mathbb{Z}/p$.

(Gegenbeispiel: Ist p keine Primzahl, so ist die entsprechende Aussage falsch. Z.B. hat für $p = 8$ das Polynom $f(x) = x^2 - 1$ die vier Lösungen $\overline{1}, \overline{3}, \overline{5}, \overline{7} \in \mathbb{Z}/8$).

Beweis : Wir beweisen die Aussage mittelt Induktion nach n:

Induktionsanfang: $n = 1$, $f(x) = a_1 x + a_0$. Dann ist $x \equiv -a_0 a_1^*$ bis auf Kongruenz die einzige Lösung, wobei $a_1^* a_1 \equiv 1 \pmod p$.

Induktionsschritt: $n > 1$. Sei x_0 eine Lösung. Dann ist

$$f(x) - f(x_0) \equiv \sum_{0 \le i \le n} a_i (x^i - x_0^i) = (x - x_0) \sum_{0 \le i \le n} a_i \frac{x^i - x_0^i}{x - x_0} = (x - x_0) g(x)$$

$g(x)$ Polynom des Grades $n-1$, mit Leitkoeffizient $a_n \equiv 0(p)$. Ist $x_1 \not\equiv x_0$ eine Lösung von $f(x_1) \equiv 0$, so gilt $\pmod p$:

$0 \equiv f(x_1) \equiv f(x_1) - f(x_0) = (x_1 - x_0) g(x_1)$. Deshalb ist $g(x_1) \equiv 0$, und es gibt nach Induktionsvoraussetzung höchstens $n-1$ Restklassen $\overline{x_i} \in \mathbb{Z}/p$ mit dieser Eigenschaft.

□

Proposition 2.20 (Eigenschaft der φ-Funktion): Für die φ-Funktion gilt:

$$\sum_{\substack{d \in \mathbb{N} \\ d \mid n}} \varphi(d) = n$$

Beweis :

Setze für $d \mid n$: $s(d) := \{i \in \mathbb{N} | 1 \le i \le n, (i,n) = d\} = \{jd | j \le \frac{n}{d}, (j, \frac{n}{d}) = 1\}$.

Dann ist $\#S(d) = \varphi(\frac{n}{d})$ und $\{1, 2, \ldots, n\} = \dot{\bigcup} S(d)$.

Nun gilt: $n = \sum_{d \mid n} \varphi(\frac{n}{d}) = \sum_{d' \mid n} \varphi(d) = \sum_{d \mid n} \varphi(d) \quad (dd' = n)$.

□

Satz/Definition 2.21 (Primitivwurzeln): Für jedes $p \in \mathbb{P}$ existieren genau $\varphi(p-1)$ Restklassen a mod p mit der Eigenschaft:

$$a^i \not\equiv 1 \pmod p \quad 1 \le i \le p-2, \quad a^{p-1} \equiv 1 \pmod p.$$

Solche $a \in \mathbb{Z}$ heißen **Primitivwurzeln** modulo p.

Beweis :

- Für jedes $a \not\equiv 0(p)$ sei $e(a) := \text{ord}_{(\mathbb{Z}/p)^*}(\overline{a}) = \min \{i \in \mathbb{N} : (a^i \equiv 1 \pmod p)\}$. Dann ist $e(a)$ ein Teiler von $p-1$
- Setze $A(d) := \{\overline{a} \in (\mathbb{Z}/p)^* | e(a) = d\}$ für $d \mid p-1$ und $f(d) := \#A(d)$.
  Wegen $(\mathbb{Z}/p)^* = \dot{\bigcup}_{d \mid n} A(d)$ ist $\sum_{d \mid n} f(d) = p - 1 \overset{2.20}{=} \sum_{d \mid p-1} \varphi(d)$.
  Es reicht also zu zeigen: $\forall\, d \mid p-1$ ist $f(d) \le \varphi(d)$ (*).
  Dann gilt sogar $f(d) = \varphi(d)$, und $f(p-1) = \varphi(p-1)$ ist die zu beweisende Aussage.
- Sei $d \mid p-1$. Ist $f(d) = 0$, so ist (*) erfüllt. Ist $f(d) > 0$, so existiert a mit $e(a) = d$,
  d.h. $a^d \equiv 1(p), \quad a^i \not\equiv 1(p)$ für $i < d$. Die Klassen von $\underbrace{a^1, a^2, \ldots, a^d}_{d \text{ viele}}$ sind alle verschieden und genügen $x^d \equiv 1$, sind also Lösungen der Kongruenz $x^d - 1 \equiv 0(p)$.
  Also folgt wegen 2.19: $A(d) \subset \{\overline{a}, \overline{a}^2, \ldots, \overline{a}^d\}$.

- Für ein $i \in \mathbb{N}$ mit $1 \leq i \leq d$ sei $g := (i,d)$. Schreibe $i = i'g, d = d'g$. Ist jetzt $g > 1$, so gilt: $(a^i)^{d'} = a^{i'gd'} = (a^d)^i \equiv 1 \pmod{p}$. Deshalb hat $\overline{a}^i$ eine Ordnung $e(a^i) \leq d' < d$, und es ist sogar $A(d) \subset \{\overline{a}^i | 1 \leq i \leq d, (i,d) = 1\}$. Also ist $f(d) \leq \varphi(d)$.

□

Definition/Korollar 2.22 (Diskreter Logarithmus): Die multiplikative Gruppe $(\mathbb{Z}/p)^*$ ist zyklisch. Die Restklasse jeder Primitivwurzel $a \pmod{p}$ erzeugt $(\mathbb{Z}/p)^*$. Ist $\overline{a}$ eine solche Primitivwurzel und $\overline{b} \in (\mathbb{Z}/p)^*$ beliebig, so $\exists!\ i \in \mathbb{N} \quad 1 \leq i \leq p-1$ mit $\overline{b} \equiv \overline{a}^i$.

Schreibe $i =: \log_{\overline{a}} \overline{b}$ und nenne es den **diskreten Logarithmus** von $\overline{b}$ bzgl. $\overline{a}$.

Es gilt z.B. $\log_{\overline{a}} \overline{b}\overline{c} \equiv \log_{\overline{a}} \overline{b} + \log_{\overline{a}} \overline{c} \pmod{p-1} \quad \overline{b}, \overline{c} \in (\mathbb{Z}/p)^*$.

Beispiel: Für $p = 13$ und $a = 2$ gilt:

$a^2 \equiv 4 \quad a^3 \equiv 8 \quad a^4 \equiv 3 \quad a^6 \equiv 12 \pmod{13}$

$\log_{\overline{2}}(a)$	12	1	4	2	9	5	11	3	8	10	7	6
a	1	2	3	4	5	6	7	8	9	10	11	12

Der diskreten Logarithmus ist z.B. sehr nützlich, wenn schnell große Zahlen multipliziert werden sollen (nicht umbedingt in $\mathbb{Z}$, sondern in allen Ringen). Dies könnte man entweder durch eine Multiplikationstabelle lösen, was aber quadratisch Platz in der Größe des Ringes benötigt. Effizienter ist es, nur eine Tabelle für den diskreten Logarithmus anzulegen, und eine Multiplikation mit Hilfe der in 2.28 genannten Formel in eine Addition umzuwandeln. D.h. um a und b zu multiplizieren, schlägt man ihre diskreten Logarithmus in der Tabelle nach, addiert diese und wandelt das Ergebnis mittels der Tabelle wieder zurück. Dieses Verfahren ist etwas langsamer als eine richtige Multiplikationstabelle, benötigt aber nur noch linearen Speicherplatz.

Korollar 2.23 (Kriterium von Euler): Sei $2 < p \in \mathbb{P}, a \in \mathbb{Z}, (a,p) = 1$. Dann gilt:

$$\exists\, x \in \mathbb{Z} \text{ mit } a \equiv x^2 \pmod{p} :\Leftrightarrow a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

Beweis : "$\Rightarrow$" $x^2 \equiv a \rightsquigarrow a^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1$.

"$\Leftarrow$" Sei y Primitivwurzel mod p, $a \equiv y^i$. Dann ist $1 \equiv a^{\frac{p-1}{2}} = y^{i\frac{p-1}{2}} \rightsquigarrow p-1 | \ i(\frac{p-1}{2}) \rightsquigarrow i$ gerade $\rightsquigarrow a = (y^{i/2})^2$.

□

Definition 2.24 (Quadratisches Symbol): Sei $2 < p \in \mathbb{P}, a \in \mathbb{Z}$. Setze

$$\left(\frac{a}{p}\right) := \begin{cases} +1 & a \not\equiv 0(p) \quad x^2 - a \equiv 0(p) \text{ hat eine Lösung} & \text{"a ist quadratischer Rest (mod } p\text{)"} \\ -1 & a \not\equiv 0(p) \quad x^2 - a \equiv 0(p) \text{ hat keine Lösung} & \text{"a ist quadratischer Nichtrest (mod } p\text{)"} \\ 0 & a \equiv 0(p) \end{cases}$$

Dies nennt man **Quadratisches Symbol** oder **Legendre-Symbol**.

Korollar 2.25 (Quadratisches Symbol): Sei $2 < p \in \mathbb{P}$. Dann gelten:

1. $$\left(\frac{n}{p}\right) = \begin{cases} +1 & i \text{ gerade} \\ -1 & i \text{ ungerade} \end{cases}$$
   falls $(n,p) = 1, n \equiv a^i, a$ Primitivwurzel mod p

   □

2. $\left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right)\left(\frac{n}{p}\right)$

   □

3. Es gibt genau $\frac{p-1}{2}$ quadratische Reste und $\frac{p-1}{2}$ quadratische Nichtreste $\pmod{p}$.

   □

   Dies folgt sofort, da die Abbildung, die jedem Element seinem Quadrat zuordnet den Kern $\{1\}$ hat.

4. $\left(\frac{n}{p}\right) \equiv n^{\frac{p-1}{2}} \pmod{p}$ falls $(n,p) = 1$

Beweis : (4): $(n^{\frac{p-1}{2}})^2 \equiv 1(p)$, also $n^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$. Nun verwende 2.23!

□

Satz 2.26 (Ergänzungssatz zum quadratischen Reziprozitätsgesetz): Sei $2 < p \in \mathbb{P}$. Es gilt:

$$\left(\frac{-1}{p}\right) = \left\{ \begin{array}{c} 1 \\ -1 \end{array} \right\} \Leftrightarrow p \equiv \left\{ \begin{array}{ll} 1 & (\mathrm{mod}\ 4) \\ 3 & (\mathrm{mod}\ 4) \end{array} \right\}$$

Beweis : Sei a Primitivwurzel $\pmod{p}$. Dann ist $a^{\frac{p-1}{2}} \equiv -1$. Ist $p \equiv 1(4)$, so gilt:

$(a^{\frac{p-1}{4}})^2 = a^{\frac{p-1}{2}} \equiv -1$, also $\left(\frac{-1}{p}\right) = +1$.

Ist $p \equiv 3(4)$, so ist $-1 \equiv a^{\frac{p-1}{2}}$ mit *ungeradem* Exponenten $\frac{p-1}{2}$, also $\left(\frac{-1}{p}\right) = -1$.

□

Satz 2.27 (Primzahlen und Restklassen modulo 4): Die Menge der Primzahlen p mit $p \equiv 1 \pmod{4}$ ist unendlich (vgl. 2.18).

Beweis : Sei $S \subset \mathbb{P}$, S endlich und für alle $p \in S$ gelte: $p \equiv 1(4)$. Wir zeigen:

$\exists\, q \in \mathbb{P}$ mit $q \equiv 1(4), q \notin S$

Setze nämlich

$$N(S) = (\prod_{p \in S} p)^2 + 1.$$ Sei q ein Primteiler von $N(S)$.

Dann ist $q \notin S$, und

$$-1 \equiv (\prod_{p \in S} p)^2 \pmod{q}.$$

Also ist $\left(\frac{-1}{q}\right) = +1$ und $q \equiv 1(4)$.

□

3 Das quadratische Reziprozitätsgesetz

Wir studieren systematisch $\left(\frac{n}{p}\right)$, wobei $2 < p \in \mathbb{P}, n = \pm \prod_{1 \le i \le p} p_i^{e_i}$ eine Primfaktorzerlegung von $n \in \mathbb{Z}$ ist. Folgende Fälle müssen betrachtet werden:

- $n = q \in \mathbb{P} \quad q \neq 2 \quad (\leftarrow 3.2)$
- $n = 2 \quad (\leftarrow 3.1)$
- $n = -1 \quad (\leftarrow 2.26)$

Satz 3.1 (Ergänzungssatz zum quadratischen Reziprozitätsgesetz):

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \left\{ \begin{array}{ll} +1 & p \equiv 1,7(8) \\ -1 & p \equiv 3,5(8) \end{array} \right.$$

Beweis : Die rechte Seite ist klar. Sei $r := \frac{p-1}{2}$. Betrachte die folgenden r Kongruenzen $\pmod p$:

$$\begin{array}{lll} p-1 & \equiv & -1 \\ 2 & \equiv & (-1)^2 2 \\ p-3 & \equiv & (-1)^3 3 \\ & \vdots & \\ \left\{ \begin{array}{ll} r \text{ gerade} & r \\ r \text{ ungerade} & r+1 \end{array} \right\} & \equiv & (-1)^r r \end{array}$$

Ihr Produkt ist $2^r r! = 2 \cdot 4 \cdots (p-1) \equiv (-1)^{\frac{r(r+1)}{2}} r!$. Also gilt $\left(\frac{2}{p}\right) \equiv 2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}\frac{p+1}{2}\frac{1}{-8}} \equiv (-1)^{\frac{p^2-1}{8}}$.

□

Satz 3.2 (Quadratisches Reziprozitätsgesetz): Seien $p,q \in \mathbb{P}$, $\#\{2,p,q\} = 3$. (D.h. die drei Zahlen sind paarweise verschieden.) Dann gilt:

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} = \left\{ \begin{array}{ll} +1 & p \text{ oder } q \equiv 1(4) \\ -1 & p \text{ und } q \equiv 3(4) \end{array} \right. .$$

Dieser Satz heißt das **quadratische Reziprozitätsgesetz** (**QRG**). Die Sätze (3.1) und (2.26) heißen die Ergänzungssätze zum quadratischen Reziprozitätsgesetz.

Beispiel 3.3 (QRG): Ist $\left(\frac{101}{127}\right) = 1$? D.h. ist 101 quadratischer Rest mod 127? Da 101 und 127 Primzahlen sind, folgt:

$$\left(\frac{101}{127}\right) \overset{101\equiv 1(4)}{=} \left(\frac{127}{101}\right) = \left(\frac{26}{101}\right) = \underbrace{\left(\frac{2}{101}\right)}_{-1}\left(\frac{13}{101}\right) \overset{3.1}{=} -\left(\frac{13}{101}\right) \overset{13\equiv 1(4)}{=} -\left(\frac{101}{13}\right) = -\left(\frac{10}{13}\right)$$

$$= -\left(\frac{2}{13}\right)\left(\frac{5}{13}\right) \overset{3.1}{=} \left(\frac{5}{13}\right) \overset{5\equiv 1(4)}{=} \left(\frac{13}{5}\right) = \left(\frac{3}{5}\right) = -1$$

D.h.: Die Gleichung $x^2 - 101 \equiv 0(127)$ hat keine Lösung.

Das quadratische Reziprozitätsgesetz wurde schon von Euler und Legendre vermutet, beide konnten es allerdings nicht beweisen. (Legendre hatte einen Beweis, der allerdings auf einer unbewiesenen Voraussetzung beruht). Inzwischen gibt es über 150 Beweise. Wir wollen hier den Beweis von Gauß demonstrieren, weil er realtiv wenige Voraussetzungen benötigt.

Beginn des Beweises von 3.2

Für $u \in \mathbb{Z}$ sei $u^* \in \{0,1,\ldots,p-1\}$ mit $u^* \equiv u \pmod p$ der **Minimalrest**.

Sei $a \in \mathbb{Z}$ mit $a \not\equiv 0 \pmod p$. Wir betrachten die Minimalreste der Zahlen $a, 2a, \ldots, \frac{p-1}{2}a$ und schreiben sie in der Form $r_1, r_2, \ldots r_s, p-r'_1, p-r'_2, \ldots, p-r'_t$, wobei $0 < r_i, r'_j < \frac{p}{2}$, $s+t = \frac{p-1}{2}$.

Lemma 3.4 (Minimalreste):

1. Die r_i sind alle verschieden.
2. Die r'_j sind alle verschieden.
3. $\{r_i\} \cap \{r'_j\} = \emptyset$

Beweis : 1. und 2. sind klar. Zu 3.:

Sei $x \in \{r_i\} \cap \{r'_j\}$. Dann sind sowohl x als auch $p-x$ Minimalreste von Zahlen der Form ab_1, ab_2 mit $b_i \in \{1,2,\ldots,\frac{p-1}{2}\}$.

Folglich muss auch $x + (p-x) = p \equiv 0(p)$ ein Minimalrest einer Zahl der Form $a(b_1+b_2) = ac \equiv 0(p)$ sein, mit $c \in \{2,3,\ldots,p-1\}$. Da $a \not\equiv 0 \pmod p$ ist, kann es kein solches c geben. Widerspruch.

□

Nach dem letzten Lemma bilden die $r_1,\dots,r_s,r_1',\dots r_t'$ eine Umordnung von $\{1,2,\dots\frac{p-1}{2}\}$. Deshalb gilt:

$$\left(\frac{a}{p}\right)\left(\frac{p-1}{2}\right)! \equiv a^{\frac{p-1}{2}}(\tfrac{p-1}{2})! = a(2a)\cdots(\tfrac{p-1}{2})a \overset{p}{\equiv} r_1\cdots r_s(p-r_1')\cdots(p-r_t') \overset{p}{\equiv} (r_1\cdots r_s r_1'\cdots r_t')(-1)^t(\tfrac{p-1}{2})!$$

Also $\left(\frac{a}{p}\right) \overset{p}{\equiv} (-1)^t$, denn $(\frac{p-1}{2})!$ enthält keinen Faktor p.

Damit ist folgender Satz bewiesen:

Satz 3.5 (Gauß): Sei $2 < p \in \mathbb{P}, a \in \mathbb{Z}, (a,p) = 1$. Dann ist

$$\left(\frac{a}{p}\right) = (-1)^t \quad t := \#\left\{u | 1 \le u \le \frac{p-1}{2}, (au)^* > \frac{p}{2}\right\}.$$

□

Definition 3.6 ($S(p,q)$): Sei $p,q \in \mathbb{P}, p \neq 2 \neq q \neq p$. Definiere:

$$S(q,p) := \sum_{1\le i\le \frac{p-1}{2}} \left[\frac{iq}{p}\right], \quad \text{wobei } [x] \text{ die Gauß-Klammer ist, d.h. der ganzzahlige Anteil der Zahl } x.$$

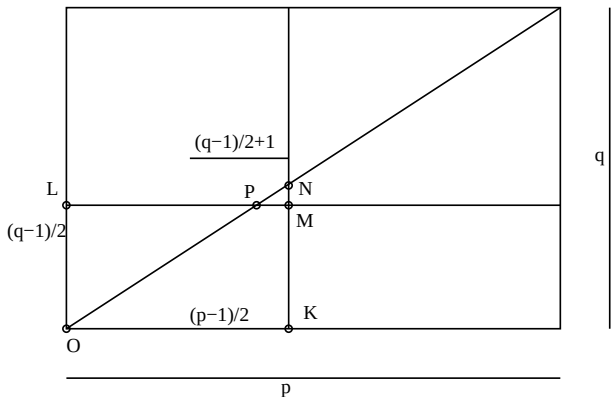
Wir wollen nun (3.2) auf Eigenschaften von $S(q,p)$ zurückführen.

Satz 3.7 (Eigenschaft von $S(q,p)$): $S(p,q) + S(q,p) = (\frac{p-1}{2})(\frac{q-1}{2})$

Der folgende Beweis stammt von Gauß:

Beweis : O.B.d.A Sei $q < p$. Dann ist $\frac{q-1}{2} < \frac{q}{p}\frac{p-1}{2} < \frac{q-1}{2} - 1$.

Betrachte folgende Zeichnung:



Auf der Geraden durch O und N liegen keine Gitterpunkte (d.h. solche mit ganzzahligen Koordinaten), da $\frac{q}{p} \in \mathbb{Q}$ die Steigung der Geraden ist, und diese vollständig gekürzt ist. Zähle jetzt die Zahl der Gitterpunkte im Rechteck $OKML$, die nicht auf den Koordinatenachsen liegen (aber auf anderen Linien liegen dürfen). Dies ist auf zwei Arten möglich:

1. Trivial: Es gibt genau $(\frac{p-1}{2})(\frac{q-1}{2})$ solche Gitterpunkte.
2. Addiere die Zahl der Gitterpunkte in den Dreiecken OKN und OPL. Dies ergibt die selbe Zahl von Punkten, da im Dreieck PMN selbst keine Punkte liegen (folgt als der Ungleichung oben). Es gilt:

$$\#(OKN) = \underbrace{\sum_{1\le i\le \frac{p-1}{2}} \left[\frac{iq}{p}\right]}_{\text{laufe auf } OK \text{ entlang und zähle die Punkte über der Position}}, \qquad \#(OPL) = \underbrace{\sum_{1\le j\le \frac{q-1}{2}} \left[\frac{jp}{q}\right]}_{\text{Laufe auf } OL \text{ und zähle die Punkte seitlich}}$$

Da diese zwei Zahlen identisch sein müssen folgt: $(\frac{p-1}{2})(\frac{q-1}{2}) = S(p,q) + S(q,p)$.

□

Rest des Beweises von (3.2): Seien p, q wie bisher, $r_1, \ldots r_s, r'_1, \ldots r'_t$ wie in (3.4) mit $a = q$.

Definiere: $R := \sum_{1 \le i \le s} r_i \quad R' := \sum_{1 \le j \le t} r'_j$.

Für $1 \le k \le \frac{p-1}{2}$ ist:

$$kq = p[\frac{kq}{p}] + u_k \quad u_k = (kq)^* = \left\{ \begin{array}{ccccc} r_i & =: & v_k & \text{sonst } v_k = 0 \\ p - r'_j & =: & w_k & \text{sonst } w_k = 0 \end{array} \right. . \quad (1)$$

Dann ist:

$$\sum v_k + tp - \sum w_k = \sum r_i + \sum r'_j = R + R' = \frac{1}{2}\left(\frac{p-1}{2}\right)\left(\frac{p+1}{2}\right) = \frac{p^2-1}{8}.$$

$$\frac{p^2-1}{8} = \sum v_k - \sum w_k + tp \quad (2)$$

Wir lassen in (1) k durch $1, 2, \ldots \frac{p-1}{2}$ laufen und summieren auf:

$$\frac{p^2-1}{8} q = p \sum_{1 \le k \le \frac{p-1}{2}} \left[\frac{kq}{p}\right] + \sum v_k + \sum w_k \quad (3)$$

(3)-(2) ergibt:

$$(q-1)\left(\frac{p^2-1}{8}\right) = pS(q,p) + 2\sum w_k - tp.$$

Daraus folgt:

$$S(q,p) \equiv t \pmod 2. \quad (4).$$

Also $\left(\frac{q}{p}\right) \overset{3.5}{=} (-1)^t = (-1)^{S(q,p)}$. Ebenso gilt: $\left(\frac{p}{q}\right) = (-1)^{S(p,q)}$, und daraus folgt:

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{S(q,p)+S(p,q)} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

□

Nun sind wir theoretisch in der Lage, $\left(\frac{a}{p}\right)$ auszuwerten. Allerdings wird dazu bisher die Primfaktorzerlegung von a benötigt, deren Berechnung sehr aufwendig ist. Im folgenden werden wir versuchen, diesen Mangel zu beseitigen:

Definition 3.8 (Jacobi-Symbol): Sei $m \in \mathbb{Z}, n \in \mathbb{N}$ ungerade und $m = \varepsilon \prod p_i^{e_i}$, bzw. $n = \prod q_j^{f_j}$ die Primfaktorzerlegung von m bzw. n mit $\varepsilon \in \{\pm 1\}$. Definiere:

$$\left(\frac{m}{n}\right) := \prod_j \left(\frac{m}{q_j}\right)^{f_j} = \prod_j \left(\frac{\varepsilon}{q_j}\right) \prod_{i,j} \left(\frac{p_i}{q_j}\right)^{e_i f_i} \in \{0, \pm 1\}.$$

$\left(\frac{m}{n}\right)$ heißt das **Jacobi-Symbol**.

Korollar 3.9 (Eigenschaften des Jacobi-Symbols): Das Jacobi-Symbol hat folgende Eigenschaften:

1. Ist $n \in \mathbb{P}$, dann sind das Jacobi-Symbol und das quadratische Symbol identisch.
2. $\left(\frac{m}{n}\right) = 0 \Leftrightarrow (m,n) > 1$ oder $m = 0$
3. $m \equiv m' \pmod n \Rightarrow \left(\frac{m}{n}\right) = \left(\frac{m'}{n}\right)$
4. $\left(\frac{mm'}{n}\right) = \left(\frac{m}{n}\right)\left(\frac{m'}{n}\right)$
5. $\left(\frac{m}{nn'}\right) = \left(\frac{m}{n}\right)\left(\frac{m}{n'}\right)$

6. Ist $(m,n)=1$, dann gilt:
$$\left(\frac{n}{m}\right)\left(\frac{m}{n}\right)=(-1)^{(\frac{m-1}{2})(\frac{n-1}{2})}=\begin{cases}+1 & m \text{ oder } n \equiv 1(4)\\ -1 & \text{falls } m \text{ und } n \equiv 3(4)\end{cases}.$$

7.
$$\left(\frac{2}{n}\right)=(-1)^{\frac{n^2-1}{8}}=\begin{cases}+1 & n\equiv 1,7(8)\\ -1 & n\equiv 3,5(8)\end{cases}$$

8.
$$\left(\frac{-1}{n}\right)=(-1)^{\frac{n-1}{2}}=\begin{cases}+1 & n\equiv 1(4)\\ -1 & n\equiv 3(4)\end{cases}$$

Beachte aber: Ist n nicht prim, so gilt nur noch: $m\equiv a^2 \pmod n \Rightarrow \left(\frac{m}{n}\right)=1$ (falls $(m,n)=1$), nicht aber die Umkehrung. Gegenbeispiel:

$n=15=5\cdot 3$. Die quadratischen Reste mod 15 sind 1,4,9,10 und 6. Davon sind nur 1 und 4 teilerfremd zu 15. Es ist aber:

$\left(\frac{8}{15}\right)=\left(\frac{8}{5}\right)\left(\frac{8}{3}\right)=\left(\frac{3}{5}\right)\left(\frac{2}{3}\right)=(-1)(-1)=1.$

Beweis : 1. bis 5. folgen direkt aus den entsprechenden Definitionen.

Zu 6.:
$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right)=\prod_{i,j}\left[\left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right)\right]^{e_if_j}=\prod_{i,j}\left[(-1)^{(\frac{p-1}{2})(\frac{q-1}{2})}\right]^{e_if_j}=(-1)^{\sum_{i,j}(\frac{p_i-1}{2})(\frac{q_j-1}{2})e_if_j}$$

Weiter gilt:
$$\sum_{i,j}(\frac{p_i-1}{2})(\frac{q_j-1}{2})e_if_j \underset{2}{\equiv} \sum_{\substack{p_i,q_j\equiv 3(4)\\ i,j}} e_if_j=\left(\sum_{p_i\equiv 3(4)}e_i\right)\left(\sum_{q_j\equiv 3(4)}f_j\right).$$

und

$m=\prod_i p_i^{e_i}\equiv 3(4) \Leftrightarrow \sum_{p_i\equiv 3(4)} e_i\equiv 1(2)$

$n=\prod_j p_j^{f_j}\equiv 3(4) \Leftrightarrow \sum_{p_j\equiv 3(4)} f_j\equiv 1(2).$

Also folgt:
$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right)=\begin{array}{rcll}1 & \Leftrightarrow & n \text{ oder } m & \equiv 1(4)\\ -1 & \Leftrightarrow & n \text{ und } m & \equiv 3(4)\end{array}.$$

7. und 8. ergeben sich ebenfalls aus den entsprechenden Eigenschaften des quadratischen Symbols.

□

4 Primzahltests

Wir kommen nun zu einem relativ neuem Gebiet der Zahlentheorie, nämlich der Frage wie man schnell entscheiden kann ob eine gegebene Zahl $n\in\mathbb{N}$ eine Primzahl ist. Diese Fragestellung ist erst seit es Computer gibt interessant geworden. Das liegt einerseits daran, daß selbst die einfachsten Algorithmen zu rechenaufwendig sind, um sie von Hand durchzuführen. Andererseits ist diese Frage gerade in der Kryptographie von besonderem Interesse. Wir notieren eine Reihe einfacher Ideen:

- Überprufe, ob die zu untersuchende Zahl in einer Primzahltabelle steht. Solche Tabellen kann man in Büchern, im Internet oder in Computeralgebrasystemen[1] finden.
- Teste alle $p\in\mathbb{P}$ mit $p\le\sqrt{n}$, ob p ein Teiler von n ist. Dies ist sehr aufwändig für große n.
- Verwende den **Fermat-Test**: Sei $a\in\mathbb{Z}$ mit $(a,n)=1$ gegeben. Ist n prim, so gilt: $a^{n-1}\equiv 1 \pmod n$. Gilt diese Kongruenz aber nicht, so kann n nicht prim sein. Es ist also möglich zu zeigen, daß n nicht prim ist ohne einen Faktor von n zu finden! Sowohl die Berechnung von (a,n) als auch von $a^{n-1}(n)$ sind "leicht" (vgl (2.14)). Deshalb gibt es eine "leichte" Methode zur Falsifikation von "n ist prim". Allerdings werden wir im Folgenden sehen, daß diese Methode nicht effektiv ist.

[1] In Computeralgebrasystemen sind typischerweise alle Primzahlen mit bis zu zwölf oder 13 Stellen tabelliert.

Definition 4.1 (Carmichael-Zahl): Eine Zahl $n \in \mathbb{N}$ heißt Carmichael-Zahl (oder **pseudo-Primzahl**), wenn gilt:

1. n ist ungerade.
2. $\forall\, a \in \mathbb{Z}$ mit $(a,n) = 1$ ist $a^{n-1} \equiv 1 \pmod{n}$
3. $n \notin \mathbb{P}$

Bemerkung (Carmichael-Zahl): In der Literatur findet man diese Definition manchmal auch ohne die dritte Bedingung.

Bemerkung (Pseudo-Primzahl): "Pseudo-Primzahl" wird nicht überall gleich definiert, und bezeichnet Zahlen, die bestimmten Primzahltests entgehen.

Der folgende Satz zeigt, daß es verhältnismäßig viele Carmichael-Zahlen gibt, d.h. daß der Fermat-Test (mit einigen zufällig gewählten a's) unsicher ist.

Satz 4.2 (Form der Carmichael-Zahlen): $n \in \mathbb{N}$ ist Carmichael-Zahl $\Leftrightarrow n = \prod_{1\le i\le s} p_i$, wobei die p_i paarweise verschiedene Primzahlen sind, s größer als eins ist und $n-1$ für alle i durch $p_i - 1$ teilbar ist.

Bevor wir diesen Satz beweisen erinnern wir noch kurz an einige Eigenschaften endlicher abelscher Gruppen:

Satz (Eigenschaften abelscher Gruppen): Sei $(G,\cdot)$ eine endliche abelsche Gruppe und $x \in G$. Dann gilt:

1. $\mathrm{ord}_G(x) := \min\{n \in \mathbb{N} \mid x^n = 1\}$
2. $e(G) := \mathrm{kgV}\{\mathrm{ord}_G(x) | x \in G\}$ e(G) heißt der **Exponent** von G.
3. Ist G zyklisch von der Ordnung n, so gilt: $e(G) = n$.
4. Ist H eine Untergruppe von G, so gilt: $e(H) \mid e(G)$ und $e(G/H) \mid e(G)$.
5. Ist p prim und $p \mid \#G$, so folgt: $p \mid e(G)$ (d.h. $p \mid \#G \Rightarrow \exists\, x \in G$ mit $\mathrm{ord}_G(x) \equiv 0 \pmod{p}$)
6. Die Primteiler von $\#G$ und $e(G)$ stimmen überein.
7. $e(G_1 \times G_2) = \mathrm{kgV}(e(G_1), e(G_2))$

Nun zum Beweis von (4.2):

Beweis : Sei n Carmichael-Zahl und $n = \prod_{1\le i\le s} p_i^{e_i}$ seine Primfaktorzerlegung. Dann gilt: $p_i^{e_i} \mid n \rightsquigarrow (\mathbb{Z}/p_i^{e_i})^*$ ist Faktorgruppe von $(\mathbb{Z}/n)^*$ (vgl. Chinesischer Restsatz). $\rightsquigarrow e((\mathbb{Z}/p_i^{e_i})^*) \mid e((\mathbb{Z}/n)^*) \mid n-1$, da n Carmichael-Zahl ist. Wäre jetzt ein $e_i > 1$, so würde gelten:

$p_i \mid e(p_i^{e_i}) = \#((\mathbb{Z}/p_i^{e_i})^*)$, also $p_i \mid e((\mathbb{Z}/p_i^{e_i})^*) \mid n-1$. D.h. $p_i \mid n$ und $p_i \mid (n-1)$, also $p_i \mid n-(n-1)$ und $p_i \mid 1$. Widerspruch.

Also ist $e_i = 1$ und $p_i - 1 = e((\mathbb{Z}/p_i)^*) \mid n-1$. Damit ist die Richtung von links nach rechts gezeigt.

"$\Leftarrow$" Sei $n = \prod_{1\le i\le s} p_i, \quad s > 1, \quad \#\{2, p_1, p_2, \ldots, p_s\} = s+1, \quad p_i - 1 \mid n-1 \forall i.$

Dann ist $e((\mathbb{Z}/n)^* = \mathrm{kgV}(e((\mathbb{Z}/p_i)^*)) = \mathrm{kgV}(p_i - 1)$ ebenfalls Teiler von $n-1$.

Also gilt für alle a mit $(a,n) = 1$: $a^{n-1} \equiv 1 \pmod{n}$

□

Beispiel 4.3 (Carmichael-Zahlen): Die kleinsten Carmichael-Zahlen sind:

$$\begin{array}{lllll} n & = & 3\cdot 11\cdot 17 & = & 561 \quad (\text{ denn 2, 10 und 16 teilen 560. }) \\ n & = & 5\cdot 13\cdot 17 & = & 1105 \quad (\text{ denn 4, 12 und 16 teilen 1004. }) \\ n & = & 7\cdot 13\cdot 19 & = & 1729 \quad (\text{ denn 6, 12 und 18 teilen 1728 .}) \end{array}$$

Die kleinste Carmichael-Zahl mit 4 Faktoren ist:

$$n = 7\cdot 11\cdot 13\cdot 41 = 41041 \quad (\text{ denn 6, 10, 12 und 40 teilen 41040. })$$

Diese Zahlen entkommen dem Fermat-Test.

Proposition 4.4 (Carmichael-Zahlen und Primteiler): Jede Carmichael-Zahl hat mindestens 3 Primteiler.

Beweis : Sei $n = pq, \quad p,q \in \mathbb{P}$. Dann gilt: $p-1 \mid n-1 = pq-1$.

Wegen $p-1 \mid (p-1)q = pq-q$ gilt also $p-1 \mid (pq-1)-(pq-q) = q-1$.

Analog gilt: $q-1 \mid p-1$, also $p = q$. Widerspuch.

□

Bemerkung 4.5 (Anzahl der Carmichael-Zahlen): Ein Satz von Alford, Granville,Pomerance (1994) besagt, daß für $x \gg 0$ gilt:

$$\#\{n \leq x \mid n \text{ ist Carmichael-Zahl } \} \geq x^{\frac{2}{7}}$$

D.h. mindestens so viele (zu viele!) n "überstehen" den Fermat-Test, der deshalb unsicher ist.

Definition 4.6 (Euler-Zeuge): Sei $n \in \mathbb{N}$ ungerade, $(a,n) = 1$. a heißt **Euler-Zeuge** (für die Zerlegbarkeit von n) wenn gilt:

$$\left(\frac{a}{n}\right) \not\equiv a^{\frac{n-1}{2}} \pmod{n}$$

Dabei kann sowohl das Jacobi-Symbol links als auch die Potenz rechts schnell berechnet werden (vgl. (3.9) und (2.14)).

Existiert ein Euler-Zeuge a zu n, so ist n zerlegbar, auch wenn wir i.a. keine Zerlegung abgeben können.

Weiter setzen wir:

$$E_n := \{\overline{a} \in (\mathbb{Z}/n)^* \mid \left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \pmod{n}\}$$

Lemma 4.7 (E_n): E_n ist Untergruppe von $(\mathbb{Z}/n)^*$.

Beweis : Wegen der Multiplikativität des Jacobi-Symbols und der Exponentation ist mit $\overline{a}, \overline{b}$ auch deren Produkt und $\overline{a^{-1}} = \overline{a}^{\varphi(n)-1} \in E_n$.

□

Satz 4.8 (Primalität und E_n): Sei $n \equiv 1(2)$. Dann gilt:

$$n \text{ prim } \Leftrightarrow E_n = (\mathbb{Z}/n)^*$$

Beweis : "⇒" gilt wegen der Euler-Kongruenz (2.23).

"⇐" Sei $E_n = (\mathbb{Z}/n)^*$. Für alle $a \in \mathbb{Z}$ mit $(a,n) = 1$ ist $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) = \pm 1$, also $a^{n-1} \equiv 1 \pmod{n}$. Deshalb ist $n \in \mathbb{P}$ oder n ist Carmichael-Zahl.

Annahme: n ist Carmichael-Zahl, d.h. $n = p_1 \cdots p_s$ mit $s \geq 3 \quad p_i - 1 \mid n-1$.

Sei $b \in \mathbb{Z}$ mit $\left(\frac{b}{p_1}\right) = -1, \quad b \equiv 1 \pmod{p_i} \quad i = 2, \ldots s$.

(b existiert nach dem Chinesischen Restsatz.)

Deshalb gilt: $b^{\frac{n-1}{2}} \overset{n}{\equiv} \left(\frac{b}{n}\right) = \left(\frac{b}{p_1}\right)\left(\frac{b}{p_2}\right)\cdots\left(\frac{b}{p_s}\right) = -1 \cdot 1 \cdots 1 = -1$.

also: $b^{\frac{n-1}{2}} \equiv -1 \pmod{n}$ und damit $b^{\frac{n-1}{2}} \equiv 1 \pmod{p_2}$.

Andererseits gilt: $b^{\frac{n-1}{2}} \equiv 1^{\frac{n-1}{2}} \equiv 1 \pmod{p_2}$. Widerspruch.

□

Korollar 4.9 (E_n): Sei $n \equiv 1(2), \quad n \notin \mathbb{P}$. Dann ist $\#(E_n) \leq \frac{\varphi(n)}{2}$ bzw. $\#\{\overline{a} | a \text{ Euler-Zeuge } \} \geq \frac{\varphi(n)}{2}$.

Beweis : E_n ist echte Untergruppe von $(\mathbb{Z}/n)^*$.

□

Primzahltest 4.10 (Primzahltest von Solovay und Strassen (1977)):

Sei $n \equiv 1(2)$. (In der Praxis $n \gg 0$)

1. Wähle $a_1, \ldots, a_r \in \{2, 3, \ldots n-1\}$ "zufällig". (Die ersten r Primzahlen sind eine gute Wahl.)
2. Teste $(a_i, n) = 1$. Falls $(a_i, n) > 1$, ist n nicht prim und wir sind fertig.
3. Ist $\underbrace{\left(\frac{a_i}{n}\right) \not\equiv a_i^{\frac{n-1}{2}} \pmod{n}}_{\text{Schnell berechenbar}}$ für ein i erfüllt, so ist n nicht prim.

Andernfalls ist die Aussage "n prim" vermutlich richtig mit einer Fehlerwahrscheinlichkeit kleiner als 2^{-r}, wenn die $\overline{a_i}$ multiplikativ unabhängig sind (Dies ist z.B. bei den ersten r Primzahlen der Fall, falls das Produkt dieser Primzahlen kleiner als n ist)[2].Nicht verwendet werden dürften z.B.: $a_1 = 2, \quad a_2 = 3, \quad a_3 = 6$, weil $\overline{a_1}, \overline{a_2} \in E_n$ bereits $\overline{a_3} \in E_n$ impliziert. Der "Versuch" a_3 liefert also keine neuen Informationen.

Beispiel 4.11 (Primzahltest von Solovay und Strassen, sowie schnelle Exponentation):

Wir wollen prüfen, ob $n = 77 = 7 \cdot 11$ eine Primzahl ist. Dazu wählen wir $a = 2$ als "Zufallszahl" und berechnen zuerst $2^{38} \pmod{77}$:

$$\begin{aligned} 2^{38} &\equiv (2^2)^{19} \equiv 4^{19} \equiv 4^{18} \cdot 4 \equiv (4^2)^9 \cdot 4 \equiv 16^9 \cdot 4 \equiv (16^2)^4 \cdot 16 \cdot 4 \equiv (25)^4 \cdot 16 \cdot 4 \\ &\equiv (25^2)^2 \cdot 16 \cdot 4 \equiv 9^2 \cdot 16 \cdot 4 \equiv 4 \cdot 16 \cdot 4 \equiv 25 \pmod{77} \end{aligned}$$

Damit gilt:

$$\left(\frac{2}{77}\right) \equiv (-1)^{\frac{77^2-1}{2}} = (-1)^{741} = -1 \not\equiv 25 \overset{\text{s.o.}}{\equiv} 2^{38} \equiv 2^{\frac{77-1}{2}} \pmod{77}.$$

Also ist 77 keine Primzahl.

□

Für große n ist dieses Verfahren allerdings immer noch aufwändig weil jeder Test die "Fehlerwahrscheinlichkeit" nur um einen Faktor 2 verkleinert. Deshalb wollen wir im folgenden den Test von Solovay und Strassen verfeinern.

Definition 4.12 (Miller-Rabin-Zeuge): Sei $0 \ll n \in \mathbb{N}, n$ ungerade. Ein **Miller-Rabin-Zeuge** (für die Zerlegbarkeit von n) ist eine Zahl $a \in \mathbb{Z}$ mit:

- $a^u \not\equiv 1 \pmod{n}$ mit $n - 1 = 2^t u$ (u ungerade)
- $a^{2^s u} \not\equiv -1 \pmod{n} \quad \forall\, s : 0 \leq s < t$

Satz 4.13 (Miller-Rabin-Zeugen und Zerlegbarkeit): Seien n, t und u wie oben. Es gilt:

1. Besitzt n einen Miller-Rabin-Zeugen, so ist n zerlegbar.
2. Ist n zerlegbar, so besitzt n Miller-Rabin-Zeugen. Insbesondere ist jeder Euler-Zeuge auch ein Miller-Rabin-Zeuge.

Für den Beweis verwenden wir den folgenden trivialen Satz:

Satz (Division und Kongruenzen): Seien $g, h, a, b \in \mathbb{Z}$ gegeben mit $g \mid a, \quad g \mid b, \quad a \equiv b \pmod{gh}$. Dann gilt:

$\frac{a}{g} \equiv \frac{b}{g} \pmod{h}$.

[2] Dabei stellt sich die Frage, was es bedeuten soll, daß eine Zahl mit einer gewissen Wahrscheinlichkeit prim ist. Man beachte, daß wir hier nur ein 'Modell' betrachten. In wie fern dieses Modell etwas mit der Wirklichkeit zu tun hat, ist eine philosophische Frage.

Beweis :

1. Sei a ein Miller-Rabin-Zeuge.

   Annahme: $n = p \in \mathbb{P}$.

   Dann ist $1 \overset{p}{\equiv} a^{p-1} = a^{(2^t u)}$. Sei s maximal mit $0 \leq s < t$ und $b := a^{(2^s u)} \not\equiv 1$. Dann gilt: $b^2 = a^{(2^{(s+1)} u)} \equiv 1$. Wegen der Primalität von p ist dann b kongruent zu -1 (modulo p), im Widerspruch zur Miller-Rabin-Eigenschaft von a.

2. Sei n zerlegbar und $\prod_{1 \leq i \leq r} p_i^{e_i}$ die Primfaktorzerlegung von n. Weiter sei $n - 1 = 2^t u$ (u ungerade).

   Wir zeigen: a Euler-Zeuge $\Rightarrow$ a Miller-Rabin-Zeuge.

   Dies gilt genau dann, wenn für die Negierungen dieser Aussagen gilt:

   $$\left\{ \begin{array}{c} (a,n) = 1 \\ a \text{ kein Miller-Rabin-Zeuge} \end{array} \right\} \Rightarrow \overline{a} \in E_n \subset (\mathbb{Z}/n)^*. \text{ d.h. } \overline{a} \text{ ist kein Euler-Zeuge .}$$

   Sei also a kein Miller-Rabin-Zeuge, d.h. $a^u \equiv 1 \pmod{n}$ oder $a^{(2^s u)} \equiv -1 \pmod{n}$ für ein s mit $0 \leq s < t$.

   1.Fall: $a^u = 1$. Dann gilt:

   $$a^{\frac{n-1}{2}} = a^{(2^{t-1} u)} \equiv (a^u)^{2^{t-1}} \equiv 1 \pmod{n}.$$

   Weiter gilt:

   $$1 = \left(\frac{1}{n}\right) = \left(\frac{a^u}{n}\right) = \left(\frac{a}{n}\right)^{u \text{ ungerade}} \overset{=}{} \left(\frac{a}{n}\right).$$

   Damit ist Fall 1 fertig.

   2.Fall: $a^{(2^s u)} \equiv -1, \quad 0 \leq s < t$.

   Für $i = 1, 2, \ldots, r$ sei $d_i := \text{ord}_{(\mathbb{Z}/p_i)^*}(\overline{a})$. Dann gilt: $d_i \not| \, 2^s u$, aber $d_i | \, 2^{s+1} u$ (vgl. Voraussetzung).

   Aus $a^{2^s u} \equiv -1 \pmod{n}$ folgt: $a^{2^s u} \equiv -1 \pmod{p_i}$, d.h.

   $(*) \quad d_i = 2^{s+1} v_i$, wobei $v_i | \, u$.

   Insbesondere sind die v_i ungerade. Wegen $d_i | \, p_i - 1$ können wir schreiben: $p_i = 2^{s+1} k_i + 1, \quad k_i \in \mathbb{N}$.

   Weiter gilt:

   $$\begin{aligned} n = \prod_{1 \leq i \leq r} p_i^{e_i} = \prod_{1 \leq i \leq r} (1 + 2^{s+1} k_i)^{e_i} = \prod_{1 \leq i \leq r} \left[1 + \binom{e_i}{1} 2^{s+1} k_i + \binom{e_i}{2} 2^{2s+2} k_i^2 + \ldots \right] \\ \equiv 1 + 2^{s+1} \sum_{1 \leq i \leq r} e_i k_i \pmod{2^{s+2}} \end{aligned}$$

   (Alle Terme, die beim letzten Schritt weggefallen sind, hatten einen Faktor 2^{2s+2}, und sind damit kongruent zu 0 (modulo 2^{s+2})).

   $\rightsquigarrow 2^{t-1} u = \frac{n-1}{2} \equiv 2^s \sum_{1 \leq i \leq r} e_i k_i \pmod{2^{s+1}}$

   $\rightsquigarrow 2^{t-1-s} \overset{u \text{ ungerade}}{\equiv} 2^{t-1-s} u \equiv \sum_{1 \leq i \leq r} e_i k_i \pmod{2}$

   Deshalb gilt (modulo n): $a^{(\frac{n-1}{2})} = a^{2^{t-1} u} = a^{(2^s u) s^{t-1-s}} \equiv (-1)^{2^{t-1-s}} = (-1)^{\sum_{1 \leq i \leq r} e_i k_i}$.

   Es bleibt $\left(\frac{a}{n}\right)$ zu berechnen.

   Zuerst ist $a^{\frac{d_i}{2}} \equiv -1 \pmod{p_i}$.

   Dann gilt:

   $$\left(\frac{a}{p_i}\right) \underset{p_i}{\equiv} a^{\frac{p_i - 1}{2}} = a^{(\frac{d_i}{2})(\frac{p_i - 1}{d_i})} \underset{p_i}{\equiv} (-1)^{\frac{p_i - 1}{d_i}} \underset{(*), \text{ da } v_i \text{ ungerade}}{=} (-1)^{\frac{p_i - 1}{2^{s+1}}} = (-1)^{k_i}$$

   Also gilt bereits: $\left(\frac{a}{p_i}\right) = (-1)^{\frac{p_i - 1}{2^{s+1}}}$. (Da beide Terme ± 1 sind, folgt aus der Kongruenz schon die Gleichheit.)

Abschließend gilt:

$$\left(\frac{a}{n}\right) = \prod_{1\le i\le r}\left(\frac{a}{p_i}\right)^{e_i} = \prod_{1\le i\le r}(-1)^{k_i e_i} = (-1)^{\sum_{1\le i\le r} k_i e_i}$$

Damit ist auch hier $\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \pmod{n}$, und die Klasse $\overline{a}$ von a (modulo n) liegt in E_n.

□

Korollar 4.14 (Anzahl der Miller-Rabin-Zeugen): Ist n ungerade und nicht prim, so besitzt n mindestens $\frac{\varphi(n)}{2}$ Miller-Rabin-Zeugen, nämlich die Zahlen, die bereits Euler-Zeugen sind.

□

Satz (Satz von Rabin (hier ohne Beweis)):

Sei $n > 9$ ungerade und zerlegbar. Dann hat n mindestens $\frac{3}{4}n \ge \frac{3}{4}\varphi(n)$ Miller-Rabin-Zeugen $\le n$.

Dieser Satz aus den Siebziger-jahren besagt also, daß wir nur halb so viele Tests benötigen, um mit der gleichen "Wahrscheinlichkeit" sagen zu können, daß n eine Primzahl ist. Darauf basiert der folgene Primzahltest:

Primzahltest 4.15 (Primzahltest von Miller-Rabin): Sei $n \gg 0$ gegeben. Wir wollen die Frage entscheiden, ob n prim ist.

1. Wähle $a_1, a_2, \ldots, a_r$ "zufällig", aber paarweise teilerfremd.
2. Teste $(n, a_i) = 1$ (Falls $(n, a) > 1$ gilt, sind wir hier bereits fertig).
3. Ist eines der a_i ein Miller-Rabin-Zeuge, so ist n zerlegbar.

   Sind alle a_i keine Miller-Rabin-Zeugen, so ist n wahrscheinlich prim, mit einer Fehlerwahrscheinlichkeit von $(\frac{1}{4})^r$.

Satz (Satz von Ankeny-Montgomery-Bach (hier ohne Beweis)):

Unter der Voraussetzung **GRH** (**Generalized Riemann Hypothesis**[3]) hat jede zerlegbare ungerade Zahl n einen Miller-Rabin-Zeugen $q \in \mathbb{P}$ mit $q < 2(\log(n))$.

In der folgenden Tabelle verdeutlichen wir, wie groß dieser Wert ist:

n	10^{10}	10^{100}	10^{1000}
$2(\log n)^2$	$1060,37954$	$106037,954$	$10603795,4$

Dies bedeuted, daß dieser Test, z.B. für eine zehnstellige Zahl n nur $\varphi(1060) = 177$ Tests machen muß um sicher zu sein, ob n eine Primzahl ist. Damit ist dieser Test nicht mehr probabilistisch!

Es gilt sogar: 2 ist Miller-Rabin-Zeuge für alle ungeraden n mit: $n \notin \mathbb{P}, n < 2^{11} - 1 = 2047$.

2 oder 3 ist Miller-Rabin-Zeuge für alle ungeraden n mit: $n \notin \mathbb{P}, n < 1.373.652 = 829 \cdot 1657$.

2, 3, 5 oder 7 ist Miller-Rabin-Zeuge für alle ungeraden n mit: $n \notin \mathbb{P}, n < 2,5 \cdot 10^{10}$, mit einer bekannten Ausnahme, nämlich $n = 3215031751 = 151 \cdot 751 \cdot 28351$.

Die Miller-Rabin-Eigenschaft gilt also viel häufiger als man zur Zeit beweisen kann.

[3] Dabei handelt es sich um eine der interessantesten, aber auch schwersten Vermutungen der Mathematik. Obwohl sie noch unbewiesen ist, wurde sie durch so viele heuristische Methoden verifiziert, daß sie allgemein als "wahr" angenommen wird. Der hier genannte Satz ist nur einer von vielen, die auf dieser Vermutung beruhen. Sollte sie tatsächlich widerlegt werden hätte dies weitreichende Auswirkungen in fast allen Zweigen der Mathematik.

Zusammenfassung:

Test	Art	Vorteile	Nachteile
Naiv (Teilersuche bis $\sqrt{n}$)	deterministisch	sicher	unbrauchbar (zu langsam)
Fermat-Test	probabilistisch	einfach	unsicher
Solovay-Strassen	probabilistisch	einfach	hohe Fehlerwahrscheinlichkeit
Miller-Rabin	probabilistisch	geringe Fehlerwahrscheinlichkeit	höherer Rechenaufwand
Miller-Rabin	deterministisch	"sicher"	höherer Rechenaufwand, beruht auf nicht bewiesener GRH.

Schlußbemerkung: Im August 2002 haben Agrawal, Kayal, Saxena einen Primzahltest vorgestellt, der deterministisch ist und nur polynomiale Komplexität hat.

5 Quadratsummen und das Waring-Problem

In diesem Kapitel wollen wir uns mit der Frage beschäftigen, welche natürlichen Zahlen sich als Summe von zwei (drei, vier, ...) Quadraten (Kuben, k-ten Potenzen) schreiben läßt. Dieses Problem bezeichnet man als das **Waring-Problem**[4]. Wir wollen uns zuerst mit folgendem Leitproblem beschäftigen:

Für welche n hat

$$(*) \qquad x^2+y^2=n$$

eine Lösung aus $\mathbb{Z}\times\mathbb{Z}$?.

Anmerkung (diophantische Gleichungen): Gleichungen, bei denen man sich nur für ganzzahlige Lösungen interessiert, bezeichnet man auch als **diophantische Gleichungen**.

Lemma 5.1 (Produkt von Quadratsummen): Mit m,n ist auch mn Summe von zwei Quadraten.

Beweis :

$$\begin{aligned}(a^2+b^2)(c^2+d^2) &= (ac+bd)^2+(ad-bc)^2\\ &= (ac-bd)^2+(ad+bc)^2\end{aligned}$$

□

Bemerkung (Produkt von Quadratsummen mit zwei Zahlen): Der Beweis des vorangegangenen Lemmas ist nur eine Übersetzung der Rechenregeln der komplexen Zahlen, denn aus $z=a+bi$, $w=c+di$ und $|z|^2|w|^2=|zw|^2=|\overline{z}w|^2$ folgt sofort obiger Beweis.

Satz 5.2 (Fermat, $\approx$ 1640): Ist $p\in\mathbb{P}, p\equiv 1 \pmod 4$, so hat (*) mit $p=n$ eine Lösung.

Beweis :

1. $\left(\frac{-1}{p}\right)=-1$, also existiert ein $x\in\mathbb{Z}$ mit $x^2\equiv 1 \pmod p$, d.h. $x^2+1=mp, \quad m\in\mathbb{N}$.

2. Deshalb hat $(\#)\quad x^2+y^2=mp$ eine Lösung (x,y) für ein geeignetes m.

   Da x,y aus $\{0,1,\ldots\frac{p-1}{2}\}$ gewählt werden kann[5] ist $m<\frac{p}{2}$. Sei m_0 ein derartiges m und minimal mit der Eigenschaft, daß (#) eine Lösung hat.

3. Annahme: $m_0>1$

   Ist $m_0 \mid x$, so gilt: $y^2\equiv 0 \pmod{m_0}$ und $g:=(y,m_0)>1$.

   $\rightsquigarrow (\frac{x}{g})^2+(\frac{y}{g})^2=(\frac{m_0}{g^2})p$.

   $\frac{m_0}{g^2}p$ ist eine ganze Zahl, und wegen $m_0<\frac{p}{2}$ ist $(m_0,p)=1$. Deshalb ist sogar $\frac{m_0}{g^2}\in\mathbb{Z}$. Dann ist $m_1:=\frac{m_0}{g^2}<m_0$ im Widerspruch zur Minimalität von m_0.

   Also gilt: $m_0 \nmid x$. Analog folgt: $m_0 \nmid y$.

[4] Genauer gesagt ist das Waring-Problem nur ein Teilproblem dieser Fragestellung.

[5] Daß x,y aus $\{0,1,\ldots p-1\}$ gewählt werden kann ist offensichtlich. Der Rest folgt, da $x^2\equiv(x-p)^2\equiv(p-x)^2 \pmod p$.

4. Finde jetzt $c,d \in \mathbb{Z}$ mit:

$$\begin{array}{rcll} x_1 & := & x - cm_0 & 0 \overset{3.}{<} |x_1| < \frac{m_0}{2} \\ y_1 & := & y - dm_0 & 0 < |y_1| < \frac{m_0}{2} \end{array}$$

Dann gilt: $x_1^2 + y_1^2 \equiv x^2 + y^2 \pmod{m_0}$ und

(##) $\quad x_1^2 + y_1^2 = m_1 m_0, \quad m_1 \leq \frac{m_0}{2}$.

5. Wir multiplizieren (#) mit (##) und erhalten

$$(xx_1 + yy_1)^2 + (xy_1 - yx_1)^2 \overset{5.1}{=} (x^2+y^2)(x_1^2+y_1^2) = m_0 m_1 p m_0 = m_0^2 m_1 p.$$

6.

$$xx_1 + yy_1 = x(x - cm_0) + y(y - dm_0) = x^2 + y^2 - m_0(cx+dy) = m_0 \underbrace{(p - cx - dy)}_{F} = m_0 F.$$

Ebenso gilt: $xy_1 - yx_1 = m_0 G$, mit $F, G \in \mathbb{Z}$.

7. Zusammen gilt:

$$m_0^2 m_1 p = (m_0 F)^2 + (m_0 G)^2 = m_0^2 (F^2 + G^2)$$

$\rightsquigarrow m_1 p = F^2 + G^2$. Also ist $0 < m_1 < m_0$, im Widerspruch zur Minimalität von m_0.

□

Definition 5.3 (Primitiv): Eine Lösung $(x,y) \in \mathbb{Z} \times \mathbb{Z}$ von $x^2 + y^2 = n$ heißt **primitiv**, falls $(x,y) = 1$, sonst **imprimitiv**.

Satz 5.4 (Summen von Quadraten und Primzahlen kongruent 3 (modulo 4)): Sei $p \in \mathbb{P}, p \equiv 3 \pmod 4, p \mid n$. Dann gilt für jede Lösung (x,y) von (*):

$p \mid x$ und $p \mid y$.

Insbesondere hat $x^2 + y^2 = p$ keine Lösung.

Beweis : Sei (x,y) Lösung von (*). Annahme: $p \nmid x$, d.h. es gilt auch $p \nmid y$. Wegen $(p,x) = 1$ existiert eine Lösung m der Kongruenz $mx \equiv y \pmod p$.

D.h. $x^2(1+m^2) \underset{p}{\equiv} x^2 + y^2 \equiv 0$.

$\rightsquigarrow 1 + m^2 \equiv 0 \pmod p \rightsquigarrow \left(\frac{-1}{p}\right) = +1$ im Widerspruch zu $p \equiv 3 \pmod 4$.

Definition 5.5 (Genauer p-Teiler): Für $p \in \mathbb{P}$ und $n \in \mathbb{N}$ sei $p^r \| n$ per Definition genau dann wahr, wenn $p^r \mid n$ und $p^{r+1} \nmid n$ erfüllt sind. Dann ist p^r der **genaue p-Teiler von** n.

Satz 5.6 (Summe zweier Quadrate): Für $n \in \mathbb{N}$ gilt: n ist genau dann Summe von zwei Quadraten, wenn alle Primteiler p von n mit $p \equiv 3 \pmod 4$ mit geradem Exponenten in n aufgehen:

$$\exists\, (x,y) \in \mathbb{Z} \times \mathbb{Z} \text{ mit } x^2 + y^2 = n \Leftrightarrow \left[\left\{ \begin{array}{c} p \in \mathbb{P}, p \mid n \\ p \equiv 3(4), p^r \| n \end{array} \right\} \Rightarrow r \equiv 0(2) \right]$$

Beweis : "⇒": Sei $n = x^2 + y^2, \quad p \mid n, \quad p \equiv 3 \pmod 4$.

Nach (5.4) gilt: $p \mid x$ und $p \mid y$, also gilt: $p^2 \mid n$.

$\rightsquigarrow \left(\frac{n}{p^2}\right) = \left(\frac{x}{p}\right)^2 + \left(\frac{y}{p}\right)^2$. Ist jetzt $\left(\frac{n}{p^2}\right) \not\equiv 0 \pmod p$, so gilt: $p^2 \| n$. Sonst folgt mit der Methode des unendlichen Abstiegs, daß $p^r \| n$ mit $r \equiv 0 \pmod 2$ für ein geeignetes $r \in \mathbb{N}$.

"⇐": Sei $n = 2^f \prod_{p_i \equiv 1(4)} p_i^{f_i} \prod_{q_j \equiv 3(4)} q_j^{2 \cdot g_j}$ die Primfaktorzerlegung von n, wobei $2, p_i, q_j \in \mathbb{P}$ alle verschieden sind.

Alle Faktoren

$$\left\{ \begin{array}{c} 2 = 1^2 + 1^2 \\ p_i \text{ nach (5.2)} \\ q_j^2 = q_j^2 + 0^2 \end{array} \right\}$$

sind Summen von zwei Quadraten. Deshalb auch n nach (5.1).

□

Als nächstes wollen wir das folgende Problem behandeln:

Für welche $n \in \mathbb{N}$ besitzt $x_1^2 + x_2^2 + x_3^2 + x_4^2 = n$ eine Lösung $(x_1, x_2, x_3, x_4) \in \mathbb{Z}^4$?

Lemma 5.7 (Produkt von Quadratsummen): Sind $m, n \in \mathbb{N}$ jeweils Summen von vier Quadraten, so kann man auch mn als Summe von vier Quadraten schreiben.

Beweis : Es gilt die Identität $(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = (z_1^2 + z_2^2 + z_3^2 + z_4^2)$, mit

$$\begin{aligned} z_1 &= x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4 \\ z_2 &= x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3 \\ z_3 &= x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4 \\ z_4 &= x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2 \end{aligned} .$$

Beachte dabei folgende Symmetrien:

- Bis auf das Vorzeichen tritt jede Kombination $x_iy_j \quad (1 \leq i, j \leq 4)$ genau einmal auf.
- Bei Ausmultiplikation der $z_1^2 + z_2^2 + z_3^2 + z_4^2$ treten 64 Terme auf. Davon sind 16 "reine" Terme, d.h. Terme der Form $(x_iy_j)^2$ und 48 Terme der Form $(x_iy_j)(x_i'y_j')$ mit $(i, j) \neq (i', j')$. Davon sind allerdings je 2 identisch, und deshalb man hat 24 Terme der Form $2(x_iy_j)(x_i'y_j')$.

Es reicht also zu sehen, daß sich die gemischten Terme wegheben. Genauer:

$\forall\ (i, j) \neq (i', j')$ kommt $2(x_iy_j)(x_i'y_j')$ genau zweimal vor, und zwar mit verschiedenen Vorzeichen. Dies kann man mittels Nachrechnen leicht verifizieren.

□

Bemerkung (Produkt von Summen von vier Quadraten): Die auftretenden Formeln erklären sich durch die Rechenregeln im **Schiefkörper**[6] $\mathbb{H}$ der Quaternionen.

$\mathbb{H} := \{a + bi + cj + dk | a, b, c, d \in \mathbb{R}\}$, wobei $\{1, i, j, k\}$ die Standardbasisbasis des 4-dimensionalen $\mathbb{R}$-Vektorraumes $\mathbb{H}$ ist. Außerdem gilt in $\mathbb{H}$, daß $i^2 = j^2 = -1$ und $ij = -ji = k$ gilt. Dies genügt, um die Multiplikation eindeutig zu machen. So gilt beispielsweise:

$ik = iij = -j$ oder $k^2 = ij(-ji) = i(-j^2)i = i^2 = -1$.

Lemma 5.8 (Summe von Quadraten): Sei $p > 2$ eine Primzahl. Dann existieren $x, y \in \mathbb{Z}, m \in N, \quad m < \frac{p}{2}$ mit

$$1 + x^2 + y^2 = mp.$$

Beweis : (Vorbemerkung: Für $p \equiv 1 \pmod 4$ geht dies sogar mit $y = 0$ (Siehe Beweis von (5.2)).

Betrachte folgende $p + 1$ Zahlen: $x^2 \quad$ mit $(0 \leq x \leq \frac{p-1}{2})$ sowie $-1 - y \quad$ mit $(0 \leq y \leq \frac{p_1}{2})$.

Die x^2 sind alle inkongruent (modulo p)[7], ebenso die $-1 - y^2$. Also existieren x, y wie oben mit $x^2 \stackrel{p}{\equiv} -1 - y^2$, d.h. $x^2 + y^2 + 1 = mp$ mit $m < \frac{p}{2}$.

□

Satz 5.9 (Summe von vier Quadraten): Jedes $n \in \mathbb{N}$ besitzt eine Darstellung als Summe von vier Quadraten[8].

[6] Schiefkörper sind Ringe, in denen multiplikative Inverse existieren, in denen die Multiplikation aber i.A. nicht kommutativ ist. Sie werden auch als Divisionsringe bezeichnet.

[7] Aus $x^2 = x'^2$ würde $x = x'$ oder $x = p - x'$ folgen. Da $p - x' \notin \{0, \ldots, \frac{p-1}{2}\}$, folgt schon $x = x'$.

[8] Dieser Satz wurde zuerst von Legendre entdeckt. Allerdings enthielt sein Beweis eine Lücke, die erst von Gauß geschlossen wurde.

Beweis : Wegen Lemma (5.7) können wir folgendes annehmen: $n = p \in \mathbb{P}, \quad p > 2$.

1. Nach Satz (5.8) existieren $x_1, x_2, x_3, x_4 \in \mathbb{Z}$ mit $\sum_{1 \le i \le 4} x_i^2 = mp, \quad m < \frac{p}{2}$.
   Sei nun m_0 ein derartiges m und minimal mit dieser Eigenschaft. Insbesondere ist m_0 kleiner als $\frac{p}{2}$.
   Annahme: $m_0 > 1$.
2. m_0 ist ungerade. Wäre nämlich m_0 gerade, dann wären 0, 2 oder 4 der x_i^2 (und damit der x_i) gerade und deshalb (nach Umnummerieren) $x_1 \equiv x_2, \quad x_3 \equiv x_4 \pmod 2$.
   Dann ist $(\frac{x_1+x_2}{2})^2 + (\frac{x_1-x_2}{2})^2 + (\frac{x_3+x_4}{2})^2 + (\frac{x_3-x_4}{2})^2 = \frac{1}{2} m_0 p$, im Widerspruch zur Minimalität von m_0.
3. Schreibe für $1 \le i \le 4$: $x_i = b_i m_0 + y_i \quad$ mit $|y_i| < \frac{m}{2}$.
4. Es existiert ein i mit $y_i \neq 0$. Wären alle $y_i = 0$, so wären auch alle $x_i \equiv 0 \pmod{m_0}$
   $\rightsquigarrow m_0^2 \mid m_0 p \rightsquigarrow m_0 \mid p$, im Widerspruch zu $m_0 < \frac{p}{2}$ oder $p \in \mathbb{P}$.
5. $\sum_{1 \le i \le 4} y_i^2 \equiv \sum_{1 \le i \le 4} x_i^2 \pmod{m_0} \equiv 0$, also $\sum_{1 \le i \le 4} y_i^2 = m_1 m_0, \quad m_1 \in \mathbb{N}, \quad m_1 < m_0$.
6. Multiplikation der Gleichungen von (1.) und (5.) ergibt:
$$\sum_{1 \le i \le 4} z_i^2 \overset{5.7}{=} \Big(\sum_{1 \le i \le 4} y_i^2\Big)\Big(\sum_{1 \le i \le 4} x_i^2\Big) = m_0^2 m_1 p.$$
7. Alle z_i sind teilbar durch m_0, denn:
$$\begin{aligned} z_1 &= x_1(x_1 - b_0 m_0) + \ldots + x_4(x_4 - b_4 m_0) \underset{m_0}{\equiv} \textstyle\sum_{1 \le i \le 4} x_i^2 \underset{m_0}{\equiv} 0 \\ z_2 &= x_1(x_2 - b_2 m_0) - x_2(x_1 - b_1 m_o) + x_3(x_4 - b_4 m_0) + x_4(x_3 - b_3 m_0) \underset{m_0}{\equiv} 0 \\ &\vdots \end{aligned}$$
8. Wegen (7.) gilt: $w_i := \frac{z_i}{m_0} \in \mathbb{Z}$. Damit folgt: $\sum_{1 \le i \le 4} w_i^2 = m_1 p$, im Widerspruch zur Minimalität von m_0, da $m_1 < m_0$.

□

Bemerkung 5.10 (Summe von drei Quadraten): Das Analogon von (5.1) bzw. (5.7) für Summen von drei Quadraten ist falsch, wie das folgende Beispiel zeigt:

$15 = 3 \cdot 5 = (1^2 + 1^2 + 1^2)(2^2 + 1^2 + 0^2)$. Aber 15 läßt sich nicht als Summe von drei Quadraten darstellen.

Satz 5.11 (Summe von drei Quadraten): Für $n \in \mathbb{N}$ sind äquivalent:

1. n besitzt keine Darstellung $n = x^2 + y^2 + z^2, \quad x, y, z \in \mathbb{Z}$.
2. n hat die Form $n = 4^a(8k + 7)$ mit $a, k \in \mathbb{N}_0$.

Beweis : "(2.) $\Rightarrow$ (1.)" bzw. "nicht (1.) $\Rightarrow$ nicht (2.)":

Sei $n = x^2 + y^2 + z^2$ und $a = \max\{i | 2^i \mid \text{ ggT } (x, y, z)\}$.

Dann ist $n = 4^a(x_1^2 + y_1^2 + z_1^2)$, wobei $x = 2^a x_1, \quad y = 2^a y_1, \quad z = 2^a z_1$, und wenigstens eines der x_1, y_1, z_1 ist ungerade. oBdA sei x_1 ungerade. Modulo 8 ist dann $x_1^2 \equiv 1, \quad y_1^2, z_1^2 \equiv 0, 1, 4$. Die Zahl $x_1^2 + y_1^2 + z_1^2$ ist dann kongruent (modulo 8) zu 1,2,3,5 oder 6.

Die Implikation "(1.) $\Rightarrow$ (2.)" bzw "nicht (2.) $\Rightarrow$ nicht (1.)" findet sich z.B. bei "Landau, Vorlesungen über elementare Zahlentheorie 1927, Reprints" oder in Büchern über algebraische Zahlentheorie. Mit unseren bisherigen Mitteln wäre ein Beweis nur schwer zu führen.

□

Ausblick 5.12 (Benachbarte Probleme):

1. Wie viele verschiedene Darstellungen als Summe von 2 (3, $\dots g$) Quadraten (Kuben, k-ten Potenzen) besitzt $n \in \mathbb{N}$?

   In Formeln: Berechne

   $r_g(n) := \#\{(x_1,\dots,x_g) \in \mathbb{Z}^g | \sum_{1\le i\le g} x_i^2 = n\}$

2. Welche $n \in \mathbb{N}$ besitzen eine Darstellung als Summe von 2,3, ... Kuben (k-ten Potenzen)? Wie viele solche Darstellungen gibt es gegebenenfalls?

3. Sei $k \in \mathbb{N}, k \ge 2$ gegeben. Gibt es eine Zahl g, so daß sich jedes $n \in \mathbb{N}$ als Summe von höchstens g k-ten Potenzen schreiben läßt?

Eng verwandt damit ist das Problem 3'.:

3'. Gibt es ein G so, daß sich fast alle Zahlen $n \in \mathbb{N}$ als Summe von höchstens G k-ten Potenzen schreiben lassen?

Setze $g(k)$ bzw $G(k)$ für die kleinstmögliche Zahl g bzw. G in 3. bzw. 3'.

3. bzw. 3'. heißt das **Waring-Problem** im engeren Sinn.

Bemerkungen 5.13 (Benachbarte Probleme): Zu den oben genannten Problemen wurde bisher folgendes herausgefunden:

1. Exakte Formeln existieren für $g \le 8$ (Siehe Hardy,Wright 20.12, Bundschuh IV §1,8). Für größere g existieren asymptotische Aussagen.

2. Zu Problem 2. gibt es bisher keine allgemeine Antwort. Es existieren lediglich einige Teilaussagen. Z.B. gilt für $k = 3$:

   $x^3 \equiv 0,1,8 \pmod 9 \quad \forall\, x \in \mathbb{Z} \rightsquigarrow (n = x^3 + y^3 \Rightarrow n \equiv 0,1,2,7,8).$

3. Im Jahre 1909 zeigte Hilbert, daß $g(k)$ für alle $k \ge 2$ existiert. Allerdings wurde keine Aussage darüber getroffen, wie groß $g(k)$ ist. Zur Zeit ist folgendes bekannt:

   $g(2) = 4$ (vgl. (5.9)).

   $g(3) = 9$ (Wieferich 1909, wobei neun Zahlen nur für $n = 23$ und $n = 239$ erforderlich sind.

   $g(4) = 19$ (Balasubramanian, Deshouillers, Dress 1985).

   $g(5) = 37$ (Chen 1964).

   Mit $g^*(k) := 2^k + [(\frac{3}{2})^k] - 2$ gilt: $g(k) = g^*(k) \quad \forall\, k \le 471.600.000$.

   Diese Gleichheit wurde mit Hilfe von Computern gezeigt. Die Zahl 471.600.000 war die größte Zahl, die mit dem Computer zu verifizieren war. Weiter ist bekannt:

   $g(k) \ge g^*(k)$. Außerdem gilt für fast alle k sogar die Gleichheit. Allerdings ist nicht bekannt für welche k die Gleichung nicht gelten könnte.

   Weiter ist $k+1 \le G(k) \le g(k)$, z.B. ist $G(3) = 7$ (Hardy, Wright).

6 Bernoulli-Zahlen und -Polynome

Die Bernoulli-Zahlen und -Polynome, die wir in diesem Kapitel behandeln, wurden zum ersten Mal von Jakob Bernoulli (1654-1705) in seinem Buch "Ars conjectardi" (Die Kunst zu vermuten 1683, posthum erschienen 1714) vorgestellt.

Erinnerung (formale Potenzreihe): Ist K ein kommutativer Ring, so heißt ein Ausdruck der Form

$$\sum_{i\in\mathbb{N}_0} a_i X^i = \sum_{i\geq 0} a_i X^i \quad (a_i \in K)$$

eine **formale Potenzreihe** über K in der Unbestimmten X. Die Menge $K[[X]]$ aller Potenzreihen über K bildet bzgl. komponentenweiser Addition und Skalarmultiplikation einen K-Modul. Der Ring $K[X]$ der Polynome in X ist ein Untermodul von $K[[X]]$. Wir definieren das Produkt $(fg)(X)$ zweier Potenzreihen $f(X) = \sum_{i\geq 0} a_i X^i$ und $g(X) = \sum_{j\geq 0} b_j X^j$ durch $(fg)(X) = \sum_{k\geq 0} c_k X^k$ mit $c_k := \sum_{\substack{i,j>0 \\ i+j=k}} a_i b_j$. Dies macht $K[[X]]$ zu einem kommutativen Ring mit $K[X]$ als Unterring.

Wir notieren einige Eigenschaften formaler Potenzreihen:

- $f(X) = \sum_{n\geq 0} a_n X^n$ ist invertierbar $\Leftrightarrow$ a_0 ist invertierbar in K.
  ("$\Rightarrow$" ist klar nach Definition von c_0. Für "$\Leftarrow$" liefert die Definition der c_k einen rekursiven Algorithmus, und es gilt: $b_0 = a_0^{-1}, b_i = \frac{-\sum a_i b_j}{a_0}$, wobei die b_i die Koeffizienten der Inversen sind.)

Ab jetzt sei $K = \mathbb{R}$ oder $K = \mathbb{C}$ und $f(X) = \sum_{i\geq 0} a_i X^i$.

- Konvergiert $\sum_{i\geq 0} |a_i| r^i$ für ein $r > 0$, so konvergiert $\sum_{i\geq 0} a_i z^i$ für alle $z \in K$ mit $|z| < r$.
  Setze $\rho(f) := \sup\{r \in \mathbb{R} | \sum_{i\geq 0} |a_i| r^i \text{ konvergiert }\}$.
  $\rho(f)$ heißt der Konvergenzradius von f. Es gilt:
  - $\rho(f) = \frac{1}{\overline{\lim}\sqrt[i]{|a_i|}}$, wobei $\frac{1}{0}$ mit unendlich und $\frac{1}{\infty}$ mit Null identifiziert wird (Abel,Hadamard). Dabei ist $\overline{\lim}$ der limes superior.
  - Sind $f, g \in K[[X]]$ mit $\rho(f), \rho(g) \geq r$, so gilt auch $\rho(f+g) \geq r, \rho(fg) \geq r$.
  - $B_r := \{z \in K | \ |z| < r\}$ (Offene Einheitskugel mit Radius r). Für $\rho = \rho(f)$ ist die Abbildung $B_\rho \to K$, $z \mapsto f(z)$, die <u>mißbräuchlich</u> ebenfalls mit f bezeichnet wird[9], differenzierbar (sogar analytisch) mit Ableitung $z \mapsto \sum_{i\geq 1} i a_i z^{i-1}$.
  - Ist $\rho(F) > 0$, und gilt $f(z) = 0 \forall\, z \in B_\rho$, so ist $f = 0$. Es genügt also, die Werte einer Potenzreihe auf einem beliebig kleinen Intervall zu kennen, um sie eindeutig zu identifizieren. Dies gilt allerdings nicht für Funktionen, für die man nur die schwächere Eigenschaft, unendlich oft differenzierbar zu sein, voraussetzt, denn die Funktion $f(z) = \left\{ \begin{array}{ll} \frac{1}{e^{(z-a)(b-z)}} & z \in (a,b) \\ 0 & \text{sonst} \end{array} \right\}$ ist ebenfalls analytisch und hat einen kompakten Träger.

Definition 6.1 (Bernoulli-Zahlen): Die k-te Bernoulli-Zahl B_k ($k \in \mathbb{N}_0$) ist definiert durch die Potenzreihe

$$F(t) := \frac{t}{e^t - 1} = \sum_{k\geq 0} \beta_k t^k =: \sum_{k\geq 0} \frac{B_k}{k!} t^k,$$

mit $B_k := k!\beta_k$. Es gilt: $F(t) \in \mathbb{Q}[[t]]$, denn mit $e^t = \sum_{k\geq 0} \frac{1}{k!} t^k$ ist auch $\frac{e^t-1}{t} = \sum_{k\geq 0} \frac{1}{(k+1)!} t^k \in \mathbb{Q}[[t]]$, und damit auch deren Inverse $F(t)$. Durch Koeffizientenvergleich im Produkt

$$1 = \frac{e^t - 1}{t} F(t) = (1 + \frac{t}{2} + \frac{t^2}{6} + \frac{t^3}{24} + \ldots)(B_0 + \frac{B_1}{1} t + \frac{B_2}{2} t^2 + \frac{B_3}{6} t^3 + \ldots)$$

erhalten wir die folgenden Werte:

$B_0 = 1, B_1 = -\frac{1}{2}, B_2 = \frac{1}{6}, B_3 = B_5 = B_7 = B_9 = 0, B_4 = -\frac{1}{30}, B_6 = \frac{1}{42}, B_8 = -\frac{1}{30}, B_{10} = \frac{5}{66}, B_{12} = -\frac{691}{2730}$.

Definition 6.2 (Bernoulli-Polynome):

Sei $\mathfrak{F}(t,X) := \frac{te^{tX}}{e^t-1} = F(t)e^{tX} = (\sum_{i\geq 0} \frac{B_i}{i!} t^i)(\sum_{j\geq 0} \frac{1}{j!}(tX)^j)$.

Schreibe dies in der Form $\mathfrak{F}(t,X) =: \sum_{k\geq 0} \frac{B_k(X)}{k!} t^k$. Dadurch wird eine Potenzreihe $B_k(X) \in \mathbb{Q}[[X]]$ bestimmt.

<u>Vorsicht</u>: $B_k \in \mathbb{Q}$, $\quad B_k(X) \in \mathbb{Q}[[X]]$. Es gilt allerdings: $B_k(0) = B_k$.

[9] Funktionen und Potenzreihen sind formal zwei verschiedene Gebilde.

Proposition 6.3 (Bernoulli-Zahlen):

1. $k \geq 3, k$ ungerade $\Rightarrow B_k = 0$
2. $$B_k = -\frac{1}{k+1} \sum_{0 \leq i < k} \binom{k+1}{i} B_i, \quad (k \geq 1)$$
3. $B_k(X)$ ist Polynom des Grades k in X. Es gilt:
$$B_k(X) = \sum_{0 \leq i \leq k} \binom{k}{i} B_i X^{k-i} = \sum_{0 \leq j \leq k} \binom{k}{j} B_{k-j} X^j.$$
4. $B_k(X+1) - B_k(X) = kX^{k-1} \quad (k \geq 1)$
5. $B_k'(X) = kB_{k-1}(X) \quad (k \geq 1)$

Beweis :

1. Es gilt:
$$F(t) - F(-t) = \frac{t}{e^t - 1} - \frac{-t}{e^{-t} - 1} = \frac{t}{e^t - 1} - \frac{te^t}{e^t - 1} = \frac{t}{e^t - 1}(1 - e^t) = -t$$
Für $k \geq 1$ ergibt ein Koeffizientenvergleich: $\frac{B_{2k+1}}{(2k+1)!} + \frac{B_{2k+1}}{(2k+1)!} = 0 \rightsquigarrow B_{2k+1} = 0$.
2. Ein Koeffizientenvergleich in $1 = (\frac{e^t-1}{t})(\frac{t}{e^t-1}) = (\sum_{i \geq 0} \frac{t^i}{(i+1)!})(\sum_{j \geq 0} \frac{B_j}{j!} t^j)$ führt für $k \geq 1$ zu:
$$0 = \sum_{\substack{i,j>0 \\ i+j=k}} \frac{1}{(i+1)!} \frac{B_j}{j!}.$$
Die Behauptung folgt durch Auflösen nach B_{k+1} und Anwenden der Rechengesetze für Binomialkoeffizienten.
3. $$\sum_{k \geq 0} \frac{B_k(X)}{k!} t^k = \mathfrak{F}(t,X) = F(t)e^{tX} = \frac{t}{e^t - 1} e^{tX} = \left(\sum_{i \geq 0} \frac{B_i}{k!} t^i \right) \left(\sum_{j \geq 0} \frac{1}{j!} X^j t^j \right)$$
Der Koeffizient von t^k auf der rechten Seite ist:
$$\sum_{\substack{i,j \geq 0 \\ i+j=k}} \frac{B_i}{i!} \frac{X^j}{j!} = \frac{1}{k!} \sum_{i+j=k} \binom{k}{i} B_i X^{k-i}$$
4. $$\sum_{k \geq 0} (B_k(X+1) - B_k(X)) \frac{t^k}{k!} = \mathfrak{F}(t,X+1) - \mathfrak{F}(t,X) = \frac{t(e^{t(X+1)} - e^{tX})}{e^t - 1} = \frac{te^{tX}}{e^t - 1}(e^t - 1) = te^{tX} = t \sum_{k \geq 0} \frac{1}{k!} X^k t^k$$
Koeffizientenvergleich des Koeffizienten von t^k führt zu:
$$\frac{B_k(X+1) - B_k(X)}{k!} = \frac{X^{k-1}}{(k-1)!} \rightsquigarrow B_k(X+1) - B_k(X) = kX^{k-1}.$$
5. Bleibt dem geneigten Leser als leichte Übung. Die Behauptung kann zum Beispiel mit 3. gezeigt werden.

Definition 6.4 ($S_k(N)$): Für $k, N \in \mathbb{N}$ sei $S_k(N) := \sum_{1 \leq i < N} i^k$.

Bemerkung (Formeln für $S_k(N)$ mit $1 \leq k \leq 4$):

$$\begin{array}{lllll} S_1(N) & = & \sum_{1\leq i<N} i & = & \frac{N(N-1)}{2} \qquad (\text{Babylon} \approx -600) \\ S_2(N) & = & \sum_{1\leq i<N} i^2 & = & \frac{N(N-1)(2N-1)}{6} \qquad (\text{Archimedes} \approx -220) \\ S_3(N) & = & \sum_{1\leq i<N} i^3 & = & (\frac{N(N-1)}{2})^2 \qquad (\text{Vieta} \approx 1600) \\ S_4(N) & = & \sum_{1\leq i<N} i^4 & = & \frac{N(N-1)(2N-1)(3N^2-3N-1)}{30} \qquad (\text{Fermat} \approx 1630) \end{array}$$

Diese Formeln folgen direkt aus dem folgenden Satz:

Satz 6.5 (Explizite Formel für $S_k(N)$): Für $k, N \in \mathbb{N}$ gilt:

$$S_{k-1}(N) = \frac{B_k(N) - B_k}{k}.$$

Beweis :

$$\begin{aligned} B_k(N) - B_k &= B_k(N) - B_k(N-1) + B_k(N-1) - B_k(N-2) + \ldots + B_k(1) - B_k(0) \\ &= k(N-1)^{k-1} + k(N-2)^{k-1} + \ldots + k0^{k-1} = k \sum_{1\leq i<N} i^{k-1} = kS_{k-1}(N) \end{aligned}$$

□

Bemerkung (Die ersten 5 Bernoulli-Polynome): Aus Proposition 6.3 (3) berechnet man leicht:

$B_1(X) = X - \frac{1}{2} \quad B_2(X) = X^2 - X + \frac{1}{6} \quad B_3(X) = X^3 - \frac{3}{2}X^2 + \frac{1}{2}X$

$B_4(X) = X^4 - 2X^3 + X^2 - \frac{1}{30} \quad B_5(X) = X^5 - \frac{5}{2}X^4 + \frac{5}{3}X^3 - \frac{1}{6}X.$

Nun erhält man leicht die Formeln aus der letzten Bemerkung.

Im Folgenden ist unser Ziel, Ausdrücke der Form $\sum_{1\leq i<N} f(i)$ zu berechnen. Dazu zeigen wir zunächst das folgende Lemma:

Lemma 6.6 (Abel-Summation): Gegeben seien zwei Folgen $(a_n)_{n\in\mathbb{N}}, (b_n)_{n\in\mathbb{N}}$ aus $\mathbb{C}$. Es gilt:

$$\sum_{1\leq n<N} a_n b_n = \sum_{1\leq n<N} A_n(b_n - b_{n-1}) + A_n b_n, \quad A_N := \sum_{1\leq i\leq n} a_i.$$

Beweis :

$$\sum_{1\leq n\leq N} a_n b_n = \sum_{1\leq n\leq N} (A_n - A_{n-1}) b_n = \sum_{1\leq n\leq N} A_n b_n - \sum_{0\leq n\leq N-1} A_n b_{n+1} \overset{A_0=0}{=} \sum_{1\leq n<N} A_n(b_n - b_{n+1}) + A_n b_n$$

Erinnerung/Ergänzung aus der Analysis (Riemann-Stieltjes-Integral):

Seien $I = [a,b] \subset \mathbb{R}, \quad f, \alpha : I \longrightarrow \mathbb{R}$

$\Delta = (x_0, \ldots, x_n)$ eine Unterteilung von I mit $a = x_0 < x_1 < \cdots < x_n = b$

$\underline{\xi} = (\xi_0, \ldots, \xi_{n-1})$ Zwischenwerte, $\quad x_i \leq \xi_i \leq x_{i+1}$ $(0 \leq i < n)$

$RS(\underline{\xi}, \Delta, f, \alpha) := \sum_{0\leq i<n} f(\xi_i)[\alpha(x_{i+1}) - \alpha(x_i)]$

Dann gilt:

(1) $\int_a^b f(x)d\alpha(x) := \lim_{|\Delta|\to 0} RS(\underline{\xi}, \Delta, f, \alpha)$

(falls dieser Limes existiert unabhängig von der Wahl der Folge von Unterteilungen Δ, deren Feinheit $|\Delta|$ gegen 0 geht, und unabhängig von der Wahl der Zwischenwerte $\underline{\xi}$).

(2) $\int_a^b f(x)d\alpha(x)$

existiert, falls f stetig ist und α beschränkte Variation hat, oder falls α stetig ist und f beschränkte Variation hat.

Eine Funktion α hat beschränkte Variation, falls eine Konstante $c > 0$ existiert, so daß für alle Unterteilungen $\delta = (x_0 \dots x_n)$ von I gilt: $\sum_{0 \le i < n} |\alpha(x_{i+1}) - \alpha(x_i)| \le c$.

Praktisch alle in der Vorlesung auftretenden Funktionen werden beschränkte Variation haben.

(3) $\int_a^b f(x)d\alpha(x)$

ist in beiden Argumenten f, α linear.

(4) Ist f stetig und α von beschränkter Variation, so gilt für alle $c \in (a,b)$:

$$\int_a^b f(x)d\alpha(x) = \int_a^c f(x)d\alpha(x) + \int_c^b f(x)d\alpha(x)$$

(5) Ist f stetig und α eine Treppenfunktion mit Sprungstellen $x_1, \dots, x_n \in (a,b)$, so gilt

$$\int_a^b f(x)d\alpha(x) = \sum_{1 \le i \le n} f(x_i)x[\alpha(x_i+) - \alpha(x_i-)].$$

Dabei ist für eine Funktion β und $x \in \mathbb{R}$:

$$\beta(x+) = \lim_{\substack{h \to 0 \\ h>0}} \beta(x+h), \quad \beta(x-) = \lim_{\substack{h \to 0 \\ h>0}} \beta(x-h).$$

(6) Ist f stetig und α stetig differenzierbar, so gilt

$$\int_a^b f(x)d\alpha(x) = \int_a^b f(x)\alpha'(x)dx.$$

(7) Ist f von beschränkter Variation und α stetig, so gilt:

$$\int_a^b f(x)d\alpha(x) = f(b)\alpha(b) - f(a)\alpha(a) - \int_a^b \alpha(x)df(x).$$

(8) Sei f stetig und α von beschränkter Variation. Für

$$F(x) := \int_a^x f(t)d\alpha(t) \quad (x \in I)$$

gelten:

(i) F hat beschränkte Variation (ist aber i.a. nicht stetig!);
(ii) $F(x+) - F(x) = f(x)[\alpha(x+) - \alpha(x)]$, $x \in [a,b)$;
(iii) $F(x) - F(x-) = f(x)[\alpha(x) - \alpha(x-)]$, $x \in (a,b]$.

Schreibe $\int_{a+}^b f(x)d\alpha(x)$ für $F(b) - F(a+)$, $\int_a^{b-} f(x)d\alpha(x)$ für $F(b-)$ etc.

Beweise und Ergänzungen finden sich z.B. in D.V. Widder, The Laplace Transform, Princeton University Press 1946, Kapitel I.

Dazu gehören insbesondere:

- Abschätzungen für $\int_a^b f(x)d\alpha(x)$, falls Abschätzungen für f und α vorliegen;
- Vertauschung von Summen mit Integralen;
- Substitutionsregel;
- uneigentliche RS-Integrale

Proposition 6.7 (Riemann-Stieltjes-Integral und Summen): Sei f monoton auf $[a,b]$, $a,b \in \mathbb{Z}$. Dann existiert ein $\theta \in [0,1]$ mit

$$\sum_{a<n\leq b} f(n) = \int_a^b f(t)dt + \theta(f(b)-f(a)).$$

Beweis : oBdA sei f monoton steigend. Schreibe $t = [t] + \{t\}, \quad \{t\} \in [0,1)$. Es ist

$$\sum_{a<n\leq b} f(n) = \int_a^b f(t)d[t]$$

$$\rightsquigarrow \sum_{a<n\leq b} f(n) - \int_a^b f(t)dt = -\int_a^b f(t)d\{t\}$$

$$\overset{(7)}{=} -f(t)\underbrace{\{t\}}_{=0}\Big|_a^b + \int_a^b \{t\}df(t) \overset{\text{MWS der Integralrechnung}}{=} \theta(f(b)-f(a)) \quad \theta \in [0,1],$$

da $\int_a^b df(t) = f(b)-f(a)$ und $0 \leq \{t\} \leq 1$ ist.

□

Beispiel (Abschätzung für $n!$): Für $f(x) = \log(x)$ erhalten wir:

$$\log n! = \sum_{1<i\leq n} \log i = (x\log x - x)|_1^n + \theta \log n = n\log n - n + 1 + \theta \log n$$

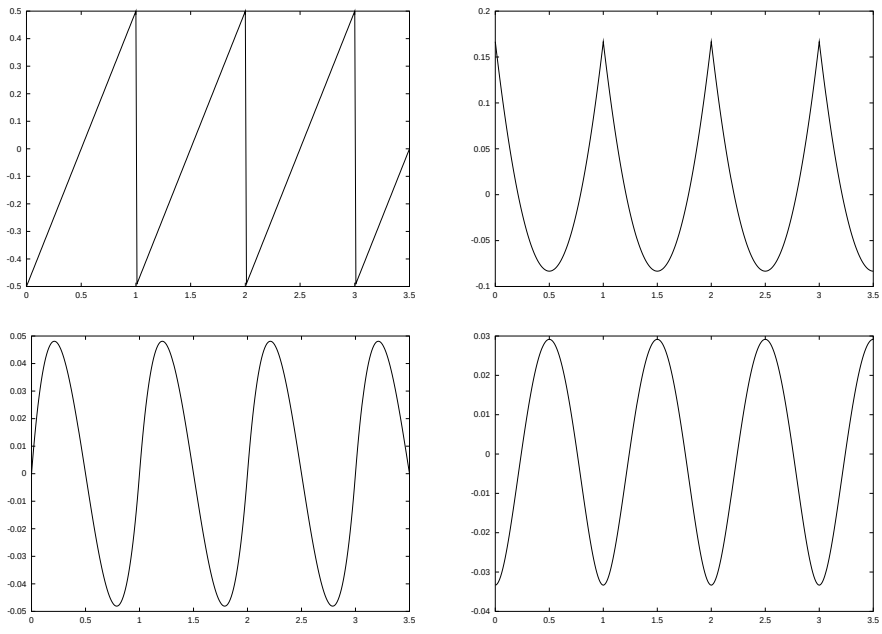
$$\rightsquigarrow n! \approx \left(\frac{n}{e}\right)^n e^{1+\theta \log n}$$

Definition/Proposition 6.8 (Bernoulli-Funktion): Für $k > 0$ sei $\beta_k : \mathbb{R} \to \mathbb{R}$ die periodische Funktion mit Periode 1, die auf $[0,1)$ mit $B_k(x)$ übereinstimmt. β_k heißt die k-te **Bernoulli-Funktion**. Es gilt:

1. Für $k \geq 2$ ist β_k stetig.
2. Für $k \geq 3$ ist β_k sogar differenzierbar.

Allgemein gelten (1.) und (2.) auf $\mathbb{R}\backslash\mathbb{Z}$ für beliebige k .

Folgende Bilder zeigen die Funktionen für $k \in \{1,2,3,4\}$ (von links nach rechts, von oben nach unten):



Beweis :

1. $B_k(1) - B_k(0) = kx^{k-1}\big|_0 = 0$, falls $k \geq 2$.
2. $B_k'(1) - B_k'(0) = (k-1)x^{k-2}\big|_0 = 0$, falls $k \geq 3$.

□

Nun wollen wir eine weitere Möglichkeit betrachten, Summen der Form $\sum_{a<n\leq b} f(n)$ zu berechnen. Dazu sei jetzt $f : [a,b] \to \mathbb{R}$ eine C^{k+1}-Funktion[10], $a,b \in \mathbb{Z}$. Dann gilt:

$$\sum_{a<n\leq b} f(n) = \int_a^b f(t)d[t] = \int_a^b f(t) - \int_a^b f(t)\underbrace{d\{t\}}_{d\beta_1(t)}$$

Dabei ist wie im Beweis von 6.7 $t = [t] + \{t\}$, $\{t\} \in [0,1)$. Mit anderen Worten: $[t]$ ist der ganzzahlige Anteil von t und $\{t\}$ ist der Nachkommaanteil von t.

Den zweiten Term bearbeiten wir weiter:

$$\int_a^b f(t)d\beta_1(t) \overset{\text{part. Integr.}}{=} f\beta_1|_a^b - \int_a^b \underbrace{\beta_1(t)}_{=\frac{1}{2}\beta_2'(t)} f'(t)dt = B_1(f(b)-f(a)) - \frac{1}{2}\int_a^b f'(t)d\beta_2(t).$$

Für das Integral im zweiten Term gilt dann:

$$\int_a^b f'(t)d\beta_2(t) = f'\beta_2\big|_a^b - \int_a^b f''(t)\beta_2(t)dt = B_2(f'(b)-f'(a)) - \frac{1}{3}\int_1^b f''(t)d\beta_3(t).$$

Wendet man dieses Verfahren k-mal an, so erhält man den folgenden Satz:

Satz 6.9 (Summenformel von Euler-MacLaurin):

$$\sum_{a<n\leq b} f(n) = \int_a^b f(t)dt + \sum_{0\leq i\leq k} (-1)^{i+1}\frac{B_{i+1}}{(i+1)!}(f^{(i)}(b) - f^{(i)}(a)) + \frac{(-1)^k}{(k+1)!}\int_a^b B_{k+1}(t)f^{(k+1)}(t)dt$$

Satz 6.10 (Summe der harmonischen Reihe): Es existiert eine Konstante $\gamma \in \mathbb{R}$, so daß für alle $N \in \mathbb{N}$ gilt:

$$H := \sum_{1\leq n\leq N}\frac{1}{n} = \log N + \gamma + \frac{1}{2N} - \frac{1}{12N^2} + \frac{\theta_N}{60N^4} \quad \theta_N \in [0,1]$$

Insbesondere gilt:

$$\lim_{N\to\infty}\Big(\sum_{1\leq n\leq N}\frac{1}{n} - \log N\Big) = \gamma, \qquad \gamma = 0,57721566\ldots$$

γ heißt die **Euler-Konstante**.

Beweis : Wir wenden (6.9) an, mit $a = 1, b = N, f(t) = \frac{1}{t}, k = 3$ und erhalten:

$$\begin{aligned}\sum_{1\leq n\leq N}\frac{1}{n} &= 1 + \log N + \frac{1}{2}(\frac{1}{N} - 1) + \frac{1}{6\cdot 2!}(\frac{-1}{N^2} + 1) - \underbrace{B_3(\ldots)}_{=0} + \frac{-1}{30\cdot 4!}(-6x^{-4})\big|_1^N - \frac{1}{4!}\int_1^N \beta_4(t)24t^{-5}dt \\ &= \log N + 1 - \frac{1}{2} + \frac{1}{12} - \frac{1}{120} + \frac{1}{2N} - \frac{1}{12N^2} + \frac{1}{120N^4} - \int_1^N t^{-5}\beta_4(t)dt.\end{aligned}$$

Es gilt: $|\beta_4(t)| \leq \frac{1}{30}$ (Einzige Extremstelle in $(0,1)$ ist der Hochpunkt $\beta_4(\frac{1}{2}) = \frac{7}{240} < |-\frac{1}{30}|$.$\beta_4$ nimmt sein Maximum also bei $\beta_4(0) = \beta_4(1) = B_4 = -\frac{1}{30}$ an.) Deshalb können wir schreiben:

[10] D.h. f ist $k+1$-fach stetig differenzierbar.

$$\int_1^N t^{-5}\beta_4(t)dt \leq \frac{1}{30}\underbrace{\int_1^N t^{-5}dt}_{\text{beschränkt}}.$$

Das Integral links ist also absolut konvergent, und es gilt:

$$\int_N^\infty |t^{-5}\beta_4(t)|dt \leq \frac{1}{30}\int_N^\infty t^{-5}dt = \frac{1}{30}\left(\frac{t^{-4}}{-4}\right)\Big|_N^\infty = \frac{1}{120N^4}.$$

D.h. es existiert ein $\theta'_N \in [-1,1]$ mit $\int_N^\infty |t^{-5}\beta_4(t)|dt = \frac{\theta'_N}{120N^4}$.

$$\rightsquigarrow \sum_{1\leq n\leq N}\frac{1}{n} - \log N = \frac{69}{120} + \frac{1}{2N} - \frac{1}{12N^2} + \frac{1}{120N^4} - \int_1^\infty t^{-5}\beta_4(t)dt + \frac{\theta'_N}{120N^4}$$

Setze $\gamma := \frac{69}{120} - \int_1^\infty t^{-5}\beta_4(t)dt, \quad \theta_N := \frac{\theta'_N+1}{2}$.

□

Nun wollen wir erneut (nach (6.7)) eine Schätzung für $n!$ zeigen. Dazu benutzen wir wieder Euler-MacLaurin mit $f(t) = \log t, k = 0$:

$$\begin{aligned}\log n! &= n\log n - n + 1 - \frac{B_1}{1}(\log n - \log 1) + \int_1^n \frac{\beta_1(t)}{t}dt \\ &= n\log n - n + \frac{1}{2}\log n + 1 + \underbrace{\underbrace{\int_1^\infty \frac{\beta_1(t)}{t}dt}_{\substack{\text{Dieses uneigentliche}\\ \text{Integral existiert.}}} - \underbrace{\int_n^\infty \frac{\beta_1(t)}{t}dt}_{=:R_n}}_{=:\frac{1}{2}\log A}\end{aligned}$$

Jetzt wollen wir zeigen, daß R_n gegen 0 geht für $n \to \infty$:

$$R_n = -\int_n^\infty \frac{\beta_1(t)}{t}dt \overset{\beta'_2=2\beta_1}{=} -\frac{\beta_2}{2t}\Big|_n^\infty - \frac{1}{2}\int_n^\infty \frac{\beta_2(t)}{t^2}dt = \frac{1}{12n} - \frac{1}{2}\int_n^\infty \frac{\beta_2(t)}{t^2}dt$$

Da $\beta_2(\frac{1}{2}) = -\frac{1}{12}$ der einzige Tiefpunkt von β_2 ist, und die Maxima am Rand globale Maxima sind, gilt: $-\frac{1}{12} \leq \beta_2(t) \leq \frac{1}{6}$. Weiter gilt: $\int_n^\infty \frac{dt}{t^2} = \frac{-1}{t}\Big|_n^\infty = \frac{1}{n}$. Aus diesen beiden Aussagen folgt mit dem Mittelwertsatz: $-\frac{1}{12n} \leq \int_n^\infty \frac{\beta_2(t)}{t^2}dt \leq \frac{1}{6n} \rightsquigarrow \frac{1}{24n} \geq -\frac{1}{2}\int_n^\infty \frac{\beta_2(t)}{t^2}dt \geq -\frac{1}{12n}$. Damit erhalten wir:

$$-\frac{1}{12n} \leq R_n - \frac{1}{12n} \leq \frac{1}{24n} \quad \rightsquigarrow 0 \leq R_n \leq \frac{1}{8n}$$

Damit gilt:

Satz 6.11 (Abschätzung für $n!$):

$$\begin{aligned}\log n! &= n\log n - n + \frac{1}{2}\underbrace{(\log n + \log A)}_{\log nA} + R_n \\ \rightsquigarrow n! &= \left(\frac{n}{e}\right)^n \sqrt{An}\cdot e^{R_n}.\end{aligned}$$

Damit ist etabliert: $\exists\, A \in \mathbb{R}^+$ mit der Eigenschaft: $\lim_{n\to\infty} \frac{n!}{\left(\frac{n}{e}\right)^n\sqrt{An}} = 1$.

Um A zu bestimmen müssen wir einige Vorbereitungen treffen:

Definition/Lemma 6.12 (Wallis-Integral): Sei $W_n := \int_0^{\frac{\pi}{2}} (\cos t)^n dt = \int_0^{\frac{\pi}{2}} (\sin t)^n dt$.

W_n heißt das Wallis-Integral. Es gilt:

1. $W_{n+1} < W_n$
2. $nW_n = (n-1)W_{n-2}$, falls $n \geq 2$

Beweis : (1.) folgt direkt aus $0 < \cos t < 1$ für $t \in (0, \frac{\pi}{2})$. Zu (2.):

$$W_n = \int_0^{\frac{\pi}{2}} \cos^{n-1} t \cos t dt \overset{\text{part. Int.}}{=} \underbrace{\cos^{n-1} t \sin t \Big|_0^{\frac{\pi}{2}}}_{=0} + (n-1) \int_0^{\frac{\pi}{2}} \sin t \cos^{n-2} \sin t dt$$

$$= (n-1) \int_0^{\frac{\pi}{2}} \cos^{n-2} t (1 - \cos^2 t) dt = (n-1) W_{n-2} - (n-1) W_n$$

□

Korollar 6.13 (Geschlossene Formel für das Wallis-Integral):

$$W_{2k} = \frac{(2k)!}{(k!2^k)^2} \frac{\pi}{2}, \quad W_{2k+1} = \frac{(k!2^k)^2}{(2k)!(2k+1)}$$

Beweis : Es gilt:

$$W_{2k} = \frac{2k-1}{2k} \cdot \frac{2k-3}{2k-2} \cdots \frac{1}{2} W_0 = \frac{(2k)!}{((2k)(2k-2)\cdots 2)^2} \underbrace{W_0}_{=\frac{\pi}{2}} = \frac{(2k)!}{(2^k k!)^2} \frac{\pi}{2}.$$

Der Beweis für W_{2k+1} erfolgt analog.

Nun sind wir in der Lage, das A aus (6.11) zu bestimmen. Es gilt:

$$\frac{n}{n+1} = \frac{W_{n+1}}{W_{n-1}} \leq \frac{W_{n+1}}{W_n} \leq 1.$$

Also ist $\lim_{n\to\infty} \frac{W_{n+1}}{W_n} = 1$. Weiter gilt:

$$\frac{W_{2k+1}}{W_{2k}} = \frac{(k!2^k)^4}{(2k)!^2(2k+1)} \frac{2}{\pi} = \frac{\left(\frac{k}{e}\right)^{4k} 2^{4k} (Ak)^2 e^{4R_k} 2}{\left(\frac{2k}{e}\right)^{4k} 2Ak\, e^{2R_{2k}} (2k+1)\, \pi} = \frac{Ak}{(2k+1)\pi} \frac{e^{4R_k}}{e^{2R_{2k}}}.$$

Für $k \to \infty$ geht dies gegen 1, ebenso wie $\frac{e^{4R_k}}{e^{2R_{2k}}}$. Also gilt:

$$A = \lim_{k\to\infty} \frac{2k+1}{k} \pi = 2\pi.$$

Damit ist folgender Satz bewiesen:

Satz 6.14 (Stirling-Formel): Es gilt:

$$n! = \left(\frac{n}{e}\right)^n \sqrt{2\pi n} e^{R_n}$$

mit $0 \leq R_n \leq \frac{1}{8n}$.

Bemerkung (Fehlerterm der Stirling-Formel): Die Euler-MacLaurin Summenformel höherer Ordnung liefert sogar:

$$\frac{1}{12n+\frac{1}{4}} \leq R_n \leq \frac{1}{12n}.$$

Deshalb ist

$$n^{\#} := \left(\frac{n}{e}\right)^n \sqrt{2\pi n} e^{\frac{1}{12n}}$$

eine noch viel bessere Annäherung an $n!$, wie auch die folgende Tabelle verdeutlicht:

n	$n!$	$\left(\frac{n}{e}\right)^n \sqrt{2\pi n}$	$n^{\#}$
2	2	$1,919\ldots$	$2,00065\ldots$
5	120	$118,019\ldots$	$120,0026\ldots$
10	3.628.800	$3.598.695,\ldots$	$3.628.810,\ldots$

Schlußbemerkung: Insbesondere können wir nun auch Terme der Form $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ näherungsweise bestimmen.

7 Die Riemannsche Zetafunktion

Erinnerung/Ergänzungen zur Analysis (Komplexer Logarithmus, absolute Konvergenz von Produkten, komplexe Exponenten):

1. Sei $l(X) = \sum_{i\geq 1}(-1)^{i+1}\frac{X^i}{i} \in \mathbb{C}[[X]]$. Dann gilt:
   (a) $\rho(l) = 1$, da $\overline{\lim}_{i\to\infty}\left|\frac{(-1)^{i+1}}{i}\right|^{\frac{1}{i}} = \overline{\lim}_{i\to\infty}\left(\frac{1}{i}\right)^{\frac{1}{i}} = 1$, denn bereits $i^{\frac{1}{i}} = e^{\left(\frac{\log i}{i}\right)}$ geht gegen eins für i gegen ∞.
   (b) $l'(X) = 1 - X + X^2 - X^3 + \ldots = \frac{1}{1+X}$
   (c) $e(l(X)) = 1 + X$

   Mit anderen Worten: Für $z \in \mathbb{C}, |z| < 1$ ist $l(z)$ die **komplexe Logarithmusfunktion** $\log 1 + z$. Dabei ist $l(z)$ nur definiert für $|z| < 1$.

2. Sei $(x_i)_{i\in\mathbb{N}}$ eine Folge aus $\mathbb{C}$. Wir sagen, daß $\prod_{i=1}^{\infty} x_i = \prod_{i\geq 1} x_i$ **absolut konvergiert**, wenn gilt:
   (a) $\lim_{i\to\infty} x_i = 1$
   (b) Es existiert ein $N \in \mathbb{N}$, so daß $|x_i - 1| < 1 \;\forall\; i > N$ und $\sum_{i>N} \log x_i$ konvergiert absolut. In diesem Fall setzen wir
   $$\prod_{i\geq 1} x_i := \prod_{1\leq i\leq N} x_i e^{\sum_{i>N}\log(x_i)}$$
   Sind (a) und (b) erfüllt, so gelten:
      i. $\prod_{i\geq 1} x_i$ ist unabhängig von der Wahl von N.
      ii. $\prod_{i\geq 1} x_i = \lim_{n\to\infty}\prod_{1\leq i\leq n} x_i$. Allerdings ist die Existenz der rechten Seite schwächer als die absolute Konvergenz. So existiert bespielsweise $\lim_{n\to\infty}\prod_{1\leq i\leq n}\frac{1}{i} = 0$, aber die Folge ist nicht absolut konvergent.
      iii. Umordnungen sind erlaubt[11].
      iv. Jedes Teilprodukt eines absolut konvergenten Produktes ist selber absolut konvergent.

3. Sei $n \in \mathbb{N}, s = x + iy,\ x,y \in \mathbb{R}$. Dann gilt: $n^s = n^{x+iy} = e^{\log n(x+iy)} = e^{x\log n} \cdot \underbrace{e^{iy}}_{\cos y + i\sin y}$. Wegen $|e^{iy}| = 1$ hängt $|n^s|$ nur von Re(s)$= x$ ab.

4. $\sum_{i\geq 1}\frac{1}{i^s}$ konvergiert $\Leftrightarrow s > 1$, falls $s \in \mathbb{R}$.

[11] Dies gilt im allgemeinen nicht, wenn nur die schwächere Bedingung an die Konvergenz gestellt wird.

Definition 7.1 (Die Riemannsche Zetafunktion): Die Riemannsche Zetafunktion ζ ist für $s \in \mathbb{C}$, $\mathrm{Re}(s) > 1$ definiert durch:

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s} = \sum_{n \geq 1} n^{-s}$$

Für diese s konvergiert diese Summe absolut.

Satz 7.2 (Euler): Für $s \in \mathbb{C}$,$\mathrm{Re}(s) > 1$ konvergiert das unendliche Produkt

$$\prod_{p \in \mathbb{P}} \left(1 - \frac{1}{p^s}\right)^{-1}$$

absolut und stimmt mit $\zeta(s)$ überein.

Beweis :

1. Sei $0 < \rho < 1$. Es existiert $C(\rho) \in \mathbb{R}$ mit: Für $|z| < \rho$ ist $|\log(1+z)| \leq C|z|$.
   Es ist nämlich
   $$|\log(1+z)| \leq \sum_{i \geq 1} \frac{|z|^i}{i} = \sum_{i \geq 1} \frac{x^i}{i} = |\log(1-x)| \quad x = |z|$$
   Wegen $\log 1 = 0, (\log(1-x))' = \frac{-1}{1-x}$ gibt es nach dem reellen Zwischenwertsatz ein $\theta \in [0,1]$ mit $\log(1-x) = \frac{-1}{1-\theta x} x$, also
   $$|\log(1+z)| \leq \underbrace{\sup_{|w| \leq \rho} \left|\frac{1}{1-w}\right|}_{=:C(\rho)} |x| \leq C(\rho)|z|.$$

2. $\prod_{p \in \mathbb{P}} \left(1 - \frac{1}{p^s}\right)^{-1}$ ist absolut konvergent $\Leftrightarrow \sum_{p \in \mathbb{P}} \log\left(1 - \frac{1}{p^s}\right)$ ist absolut konvergent. Für $\mathrm{Re}(s) > 1$ ist $|p^{-s}| < \frac{1}{2}$, also gilt mit $C = C(\frac{1}{2})(= 2)$:
   $$\sum_{p \in \mathbb{P}} \left|\log\left(1 - \frac{1}{p^s}\right)\right| \leq C \sum_{p \in \mathbb{P}} |p^{-s}| \leq C \sum_{n \in \mathbb{N}} |n^{-s}| \leftarrow \text{absolut konvergent}$$

3. $\mathbb{P}(x) := \{p \in \mathbb{P} | p \leq x\}$, $\mathbb{N}(x) := \{n \in \mathbb{N} | n$ hat nur Primfaktoren aus $\mathbb{P}(x)\}$

   $$\prod_{p \in \mathbb{P}(x)} (1 - p^{-s})^{-1} = \prod_{p \in \mathbb{P}(x)} (1 + p^{-s} + p^{-2s} + \ldots) = \sum_{n \in \mathbb{N}(x)} n^{-s} \quad \text{(Eindeutige Primfaktorzerlegung)}$$

   Lassen wir x gegen ∞ gehen, so geht die linke Seite gegen $\prod_{p \in \mathbb{P}} (1 - p^{-s})^{-1}$, und für die rechte Seite gilt:

   $$\left|\zeta(s) - \sum_{n \in \mathbb{N}(x)} n^{-s}\right| = \left|\sum_{n \in \mathbb{N} \setminus \mathbb{N}(x)} n^{-s}\right| \leq \left|\sum_{n \in \mathbb{N} \setminus \mathbb{N}(x)} n^{-\mathrm{Re}(s)}\right| \leq \sum_{n > x} n^{-\mathrm{Re}(s)} \xrightarrow{x \to \infty} 0$$

   $$\rightsquigarrow \prod_{p \in \mathbb{P}} (1 - p^{-s})^{-1} = \zeta(s).$$

Probleme 7.3 (Wahrscheinlichkeit für Teilerfremdheit und quadratfreiheit):

1. Wie groß ist die Wahrscheinlichkeit, daß zwei zufällig gewählte natürliche Zahlen teilerfremd sind? D.h. existiert der folgende Grenzwert, und welchen Wert besitzt er gegebenenfalls?
   $$\lim_{x \to \infty} \frac{\#\{(m,n) \in \mathbb{N}^2 | (m,n) = 1, \quad m,n \leq x\}}{\#\{(m,n) \in \mathbb{N}^2 | m,n \leq x\}}$$

2. Wie groß ist die Wahrscheinlichkeit, daß eine zufällig gewählte Zahl n quadratfrei ist? D.h. welchen Wert hat der folgende Grenzwert, falls er existiert?

$$\lim x \to \infty \frac{\#\{n \in \mathbb{N} | n \leq x, n \text{ ist quadratfrei}\}}{\#\{n \in \mathbb{N} | n \leq x\}}$$

Zu diesen Problemen machen wir die folgenden heuristischen Überlegungen:

1.
$$(m,n) = 1 \Leftrightarrow \begin{cases} (m,n) & \not\equiv & (0,0) & (\text{mod } 2) \\ (m,n) & \not\equiv & (0,0) & (\text{mod } 3) \\ & \cdots & & \\ (m,n) & \not\equiv & (0,0) & (\text{mod } p) \quad \forall\, p \in \mathbb{P} \end{cases}$$

Die Bedingung $(m,n) \not\equiv (0,0) \pmod{p}$ ist in $p^2 - 1$ von p^2 Fällen erfüllt, also mit Wahrscheinlichkeit $\frac{p^2-1}{p^2} = 1 - p^{-2}$. Wegen der Unabhängigkeit der Bedingungen für verschiedene p's (vgl. Chinesischer Restsatz) ist also $P((m,n) = 1) = \prod_{p \in \mathbb{P}} (1 - p^{-2}) = \zeta(2)^{-1}$ (?)

2. Analog folgt:
$$n \text{ quadratfrei } \Leftrightarrow \begin{cases} n & \not\equiv & 0 & (\text{mod } 2)^2 \\ n & \not\equiv & 0 & (\text{mod } 3)^2 \\ & \cdots & & \\ n & \not\equiv & 0 & (\text{mod } p)^2 \quad \forall\, p \in \mathbb{P} \end{cases}$$

$\rightsquigarrow P(n \text{ quadratfrei }) = \prod_{p \in \mathbb{P}} (1 - p^{-2}) = \zeta(2)^{-1}$ (?)

Allgemein gilt:

$$P((n_1 \dots n_k) = 1) = \zeta(k)^{-1}$$
$$P(n \text{ enthält keine } k\text{-ten Potenzen}) = \zeta(k)^{-1} (?)$$

Die Fragezeichen deuten an, daß es sich im Moment nur um Plausibilitätsbetrachtungen handelt. Später werden wir diese Sachverhalte exakt beweisen.

Satz 7.4 (Wert der Zeta-funktion an der Stelle 2):

$$\zeta(2) = \frac{\pi^2}{6}$$

Dieser Satz stammt von Euler aus dem Jahre 1735. Der folgende Beweis wurde allerdings erst 1985 von Calabi gefunden:

Beweis : Sei $I = [0,1], I_\varepsilon = [0, 1-\varepsilon]$. Wir berechnen $\int_I \int_I \frac{1}{1-x^2y^2} dxdy$ auf zwei verschiedene Weisen:

1. $\frac{1}{1-x^2y^2} dxdy = 1 + x^2y^2 + x^4y^4 + \dots$ absolut konvergent für $(x,y) \in I_\varepsilon$

$$\rightsquigarrow \int_{I_\varepsilon} \int_{I_\varepsilon} \frac{1}{1-x^2y^2} dxdy = \sum_{i \geq 0} \int_{I_\varepsilon} \int_{I_\varepsilon} x^{2i} y^{2i} dxdy = \sum_{i \geq 0} \frac{(1-\varepsilon)^{2i+1}}{(2i+1)^2}$$
$$\xrightarrow{\varepsilon \to 0} \int_I \int_I \frac{1}{1-x^2y^2} dxdy = \sum_{i \geq 0} \frac{1}{(2i+1)^2} = \sum_{n \in \mathbb{N}} \frac{1}{n^2} - \sum_{n \in \mathbb{N}} \frac{1}{(2n)^2} = \zeta(2)(1 - \frac{1}{4})$$

Um den Beweis dieses Satzes fortzusetzen brauchen wir das folgende Lemma:

Lemma 7.5 (Bijektion von Quadrat zum Dreieck): Sei $\triangle = \{(u,v) \in \mathbb{R}^2 | u,v \geq 0, u+v \leq \frac{\pi}{2}\}$ mit Innerem $\mathring{\triangle} = \{(u,v) \in \mathbb{R}^2 | u,v > 0, u+v < \frac{\pi}{2}\}$. Dann ist die Abbildung

$$\varphi : (u,v) \mapsto \left(\frac{\sin u}{\cos v}, \frac{\sin v}{\cos u} \right)$$

eine Bijektion von $\mathring{\triangle}$ mit $\mathring{I} \times \mathring{I} = (0,1) \times (0,1)$.

Beweis : Der Cosinus ist auf $(0, \frac{\pi}{2})$ streng monoton fallend. Dehalb folgt aus $v < \frac{\pi}{2} - u$:

$$\cos(v) > \cos(\frac{\pi}{2} - u) = \sin u, \text{ d.h. } \frac{\sin u}{\cos v} < 1.$$

Analog folgt: $\frac{\sin v}{\cos u} < 1$. Wir setzen $x := \frac{\sin u}{\cos v}, y := \frac{\sin v}{\cos u}$ und erhalten:

$$\begin{aligned}
&\sin^2 u = x^2 \cos^2 v, \quad \sin^2 v = y^2 \cos^2 u \rightsquigarrow 1 = \cos^2 v + \sin^2 v = \cos^2 v + y^2 \cos^2 u \\
&\rightsquigarrow \cos^2 v = 1 - y^2 \cos^2 u = 1 - y^2(1 - x^2 \cos^2 v) \rightsquigarrow (1 - x^2 y^2) \cos^2 v = 1 - y^2 \\
&\rightsquigarrow \cos v = \sqrt{\frac{1 - y^2}{1 - x^2 y^2}} \rightsquigarrow v = \arccos \sqrt{\frac{1 - y^2}{1 - x^2 y^2}}
\end{aligned}$$

Analog folgt: $v = \arccos \sqrt{\frac{1-x^2}{1-x^2y^2}}$. D.h. $\varphi^{-1}(x,y) = (u,v)$.

□

Nun setzen wir den Beweis von (7.4) fort:

2. Mit Bezeichnungen wie in (7.5) ist

$$\begin{pmatrix} \frac{\partial x}{\partial u} & \frac{\partial x}{\partial v} \\ \frac{\partial y}{\partial u} & \frac{\partial y}{\partial v} \end{pmatrix} = \begin{pmatrix} \frac{\cos u}{\cos v} & \frac{\sin u \sin v}{\cos^2 v} \\ \frac{\sin v \sin u}{\cos^2 u} & \frac{\cos v}{\cos u} \end{pmatrix}$$

   mit Determinante $1 - x^2y^2$. Nun gilt:

$$\int_I \int_I \frac{dx\, dy}{1 - x^2 y^2} = \int_\triangle \frac{\det(\ldots) du\, dv}{1 - x^2 y^2} = \int_\triangle du\, dv = \text{Fläche des Dreiecks} = \frac{\pi^2}{8}$$

3. Also gilt $\frac{3}{4}\zeta(2) = \frac{\pi^2}{8}$, d.h. $\zeta(2) = \frac{\pi^2}{6}$.

□

Satz 7.6 (Wert der Zeta-Funktion für natürliche Zahlen): Sei $k \in \mathbb{N}$ gerade. Dann gilt:

$$\zeta(k) = -\frac{1}{2} \frac{(2\pi i)^k}{k!} B_k$$

Beweis :

1. Es gilt:

$$\begin{aligned}
z \cot z &= z \frac{\cos z}{\sin z} = z \frac{\frac{e^{iz} + e^{-iz}}{2}}{\frac{e^{iz} - e^{-iz}}{2i}} = iz \frac{e^{iz} + e^{-iz}}{e^{iz} - e^{-iz}} = iz \left(\frac{e^{2iz} + 1}{e^{2iz} - 1} \right) = iz + \frac{2iz}{e^{2iz} - 1} \\
&= izF(2iz) = iz + \sum_{k \geq 0} (2i)^k B_k \frac{z^k}{k!} = \sum_{\substack{k \geq 0 \\ k \neq 1}} (2i)^k \frac{B_k}{k!} z^k.
\end{aligned}$$

   Dies ist eine alternative Definition der B_k (ohne B_1).

   Erinnerung/Ergänzung 7.7 (Sinus/logarithmische Ableitung):

   - Eine mögliche Definition der **Sinus**-Funktion ist:

$$\sin z = z \prod_{n=1}^{\infty} \left(1 - \frac{z^2}{n^2 \pi^2} \right), \quad z \notin \mathbb{Z}\pi$$

     ist abolut konvergentes Produkt und normal konvergent auf abgeschlossenen Kreisscheiben, die $\mathbb{Z}\pi$ nicht treffen.

- Sei f eine stetig differenzierbare Funktion ohne Nullstellen. Die **logarithmische Ableitung** Df ist definiert durch:
$$Df := \frac{f'}{f} \underset{f>0}{=} (\log f)'.$$
Es gilt:
  - $D(cf) = D(f)$ für alle Konstanten $c \in \mathbb{R}$.
  - $D(f \cdot g) = D(f) + D(g)$
  - $D(\prod_{1\le i\le n} f_i) = \sum_{1\le i\le n} D(f_i)$
  - $D(\prod_{i\ge 1} f_i) = \sum_{i\ge 1} D(f_i)$ für unendliche, normal und absolut konvergente Produkte.

2. Weiter gilt nun:
$$\begin{aligned}
\sin z &= z\prod_{n=1}^{\infty}\left(1-\frac{z^2}{n^2\pi^2}\right)\\
\overset{D}{\rightsquigarrow} \cot z &= \frac{1}{z}+\sum_{n\ge 1}\frac{-2z}{n^2\pi^2-z^2}\\
\overset{\cdot z}{\rightsquigarrow} z\cot z &= 1-2\sum_{n\ge 1}\frac{z^2/n^2\pi^2}{1-z^2/n^2\pi^2}\\
\rightsquigarrow z\cot z &= 1-2\sum_{n\ge 1}\sum_{k\ge 1}\left(\frac{z^2}{n^2\pi^2}\right)^k \leftarrow \text{ absolut konvergente Doppelsumme, falls } z\notin\mathbb{Z}\pi\\
&= 1-2\sum_{k\ge 1}\pi^{-2k}\underbrace{\sum_{n\ge 1}\frac{1}{n^{2k}}}_{\zeta(2k)}z^{2k} = 1-2\sum_{\substack{k\ge 2\\ k \text{ gerade}}}\pi^{-k}\zeta(k)z^k
\end{aligned}$$

3. Koeffizientenvergleich der Ergebnisse von 1. und 2. liefert für gerade k:
$$\begin{aligned}
-2\pi^{-k}\zeta(k) &= (2i)^k\frac{B_k}{k!}\\
\rightsquigarrow \zeta(k) &= -\frac{1}{2}\frac{(2\pi i)^k}{k!}B_k
\end{aligned}$$

□

Beispiel (Wert der Zeta-Funktion an den Stellen 2, 4 und 6):

$$\begin{array}{lllll}
k=2: & \zeta(2) & = & -\frac{1}{2}\frac{(2\pi i)^2}{2}\frac{1}{6} & = \frac{\pi^2}{6}\\
k=4: & \zeta(4) & = & \dots & = \frac{\pi^4}{90} \quad (B_4=\frac{-1}{30})\\
k=6: & \zeta(6) & = & \dots & = \frac{\pi^6}{945} \quad (B_6=\frac{1}{42})
\end{array}$$

Korollar 7.8 (Vorzeichen der Bernoulli-Zahlen):

Für jedes gerade $k>0, k=2l$ ist $B_k \neq 0$ und sgn(B_k) = $(-1)^{l-1}$.

□

Die Folge $\zeta(k)$ konvergiert rasch gegen 1, wie man an der folgenden Tabelle sieht:

k	2	3	4	5	10
$\zeta(k)$	1.64493…	1.20205…	1.08232…	1.03692…	1.00099…

Satz 7.9 (Näherungsformel für die Bernoulli-Zahlen): Sei $l \in \mathbb{N}$. Dann gilt:
$$B_{2l} \approx -2\frac{(2l)!}{(2\pi i)^{2l}} = (-1)^{l-1}2\frac{(2l)!}{(2\pi)^{2l}}$$

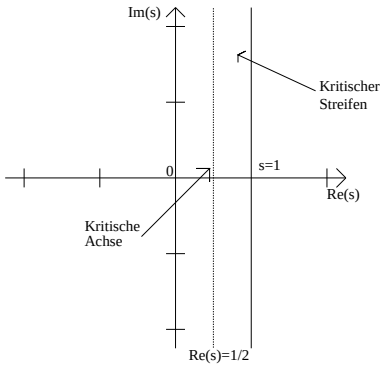


Abbildung 1: Kritischer Streifen und kritische Achse.

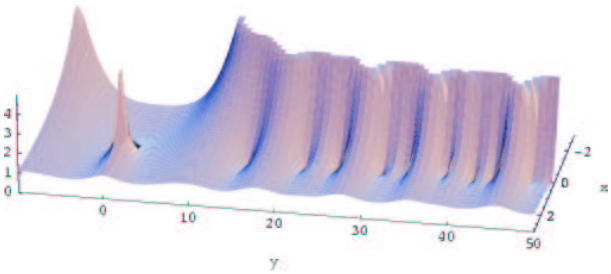


Abbildung 2: Dieses Bild zeigt den Betrag der Riemannschen Zeta-Funktion, und stammt von der Seite *www.maths.ex.ac.uk/∼mwatkins/zeta/ssm.htm*. Dort befinden sich auch eine Reihe weiterer interessanter Bilder zur Primzahlverteilung und zur Riemannschen Zeta-Funktion.

Ergänzungen 7.10 (zur Zeta-Funktion):

- Wir wissen bereits: $\zeta(2k) = \pi^{2k} \cdot$ rationale Zahl, $\quad k \in \mathbb{N}, \pi$ transzendent[12].

  Allerdings ist über die Werte der Zeta-Funktion für ungerade Werte fast gar nichts bekannt. Die einzige sichere Information ist, daß $\zeta(3)$ irrational ist (Apéry 1977).

- $\zeta(s)$ besitzt eine meromorphe Fortsetzung auf $\mathbb{C}$ mit einem Pol der Ordnung 1 an $s = 1$ und keinen weiteren Singularitäten. Es ist $\mathrm{Res}_{s=1}\zeta(s) = 1$, d.h. die Funktion $\zeta(s) - \frac{1}{s-1}$ besitzt in $s = 1$ eine hebbare Singularität.

- Die **Gamma-Funktion**
$$\Gamma(s) := \int_0^\infty t^{s-1}e^{-t}dt, \quad \mathrm{Re}(s) > 0$$
besitzt eine meromorphe Fortsetzung auf $\mathbb{C}$ und genügt den folgenden Funktionalgleichungen:
  - $\Gamma(s+1) = s\Gamma(s)$
  - $\Gamma(s) =$ trigonometrischer Faktor $\cdot\, \Gamma(1-s)$
  - $\Gamma(n+1) = n!, \quad n \in \mathbb{N}$

  Für
$$Z(s) := \pi^{-s/2}\Gamma(\frac{s}{2})\zeta(s)$$
gilt: $Z(1-s) = Z(s)$. Mit Hilfe dieser Funktion können wir die Zeta-Funktion deshalb auch für negative Werte definieren und erhalten $\zeta(1-k) = (-1)^{k+1}\frac{B_k}{k}$ für $k \in \mathbb{N}$, d.h. $\zeta(1-k) = -\frac{B_k}{k}$ für $k > 1$.

  So ist beispielsweise $\zeta(0) = -\frac{1}{2}$ und $\zeta(-2k) = 0, k \in \mathbb{N}$. Weiter können wir den nicht konvergenten Term $\sum_{n=1}^\infty n^{k-1}, k \in \mathbb{N}$ mit $\zeta(1-k)$ identifizieren und ihm so einen Wert ungleich unendlich zuweisen. Besonders im Bereich der p-adischen Zahlen sind solche Betrachtungen sinnvoll.

- Aus der Tatsache, daß ζ keine Nullstelle mit Re(s) = 1 hat, erschließt man:
$$\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\log x}} = 1$$
Diese Aussage heißt **Primzahlsatz**, ($\pi(x)$ ist definiert durch $\pi(x) = \#\{p \in \mathbb{P} | p \le x\}$). Sie wurde gleichzeitig 1896 von Hadamard und de la Vallée Poussin bewiesen.

[12] Eine Zahl heißt transzendent, wenn sie nicht Nullstelle eines Polynoms mit rationalen Koeffizienten ist.

Jeder Streifen nahe 1, in dem keine Nullstellen liegen, liefert eine Abschätzung für den Fehlerterm $|\pi(x) - \frac{x}{\log x}|$. Besonders interessant ist hier die **Riemannsche Vermutung**: Alle nichttrivialen Nullstellen s von ζ (d.h. alle Nullstellen die nicht die Form $s = -2k, k \in \mathbb{N}$ haben) genügen Re(s) = $\frac{1}{2}$, d.h. sie liegen auf der sogenannten **kritischen Achse**.

Ein Beweis dieser Vermutung ist allerdings noch nicht in Sicht. Bekannt sind lediglich die folgenden schwächeren Aussagen:

- Es gibt unendlich viele Nullstellen auf der kritischen Achse.
- Mindestens 40% der Nullstellen im **kritischen Streifen** $\{s \in \mathbb{C} | 0 \leq \mathrm{Re}(s) \leq 1\}$ liegen auf der kritischen Achse.
- Zu jedem $\delta > 0$ existieren nur endlich viele Nullstellen s im kritischen Streifen mit $|\mathrm{Re}(s) - \frac{1}{2}| > \delta$.

8 Die Sätze von Tschebyschew zur Primzahlverteilung

Unser Ziel ist es nun, eine Abschätzung für $\pi(x) := \#\{p \in \mathbb{P} | p \leq x\}, x \in \mathbb{R}$ der Form $a\frac{x}{\log(x)} \leq x \leq b\frac{x}{\log(x)}$ zu finden, wobei $a, b \in \mathbb{R}$, a möglichst groß und b möglichst klein sein soll.[13]

Proposition 8.1 (Vielfachheiten und Fakultäten): Sei $n \in \mathbb{N}, n! = \prod_{p \in \mathbb{P}} p^{v_p}, v_p = v_p(n!)$ die Vielfachheit von p in $n!$. Dann gilt:

1. $$v_p = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \ldots \quad \leftarrow \text{endliche Summe}$$
2. Für festes p sei $n = \sum_{i \geq 0} a_i p^i$ mit $a_i \in \{0, 1, \ldots, p-1\}$ die p-adische Entwicklung und $l_p = \sum_{i \geq 0} a_i$ die p-adische Quersumme. Dann gilt:
$$v_p = \frac{n - l_p(n)}{p-1}.$$
3. Es gilt die folgende Ungleichung:
$$\frac{n}{p} - 1 < v_p < \frac{n}{p} + \frac{n}{p(p-1)}.$$

Beispiel (Vielfachheiten und Fakultäten): Wir berechnen $v_2(19!)$ auf zwei Arten:

- $v_2(19!) = \left[\frac{19}{2}\right] + \left[\frac{19}{4}\right] + \left[\frac{19}{8}\right] + \left[\frac{19}{16}\right] = 9 + 4 + 2 + 1 = 16$
- $19 = 16 + 2 + 1 \rightsquigarrow l_2(19) = 3 \rightsquigarrow v_2(19!) = \frac{19-3}{2-1} = 16$

Beweis :

1. Unter den Faktoren $1, 2, \ldots n-1, n$ von $n!$ sind
$$\begin{array}{ll} p, 2p, \ldots & \left[\frac{n}{p}\right] p \text{ durch } p \text{ teilbar}, \\ p^2, 2p^2, \ldots & \left[\frac{n}{p^2}\right] p^2 \text{ durch } p^2 \text{ teilbar}, \\ \vdots & \\ p^r, 2p^r, \ldots & \left[\frac{n}{p^r}\right] p^r \text{ durch } p^r \text{ teilbar}, \end{array}$$
Deshalb gibt es genau $\left[\frac{n}{p^r}\right] - \left[\frac{n}{p^{r+1}}\right]$ viele $i \in \{1, 2, \ldots, n\}$ mit $p^r \| i$. Also ist die Zahl der Faktoren p in $n!$ gegeben durch
$$\begin{aligned} v_p(n!) &= 0\left(\left[\frac{n}{1}\right] - \left[\frac{n}{p}\right]\right) + 1\left(\left[\frac{n}{p}\right] - \left[\frac{n}{p^2}\right]\right) + 2\left(\left[\frac{n}{p^2}\right] - \left[\frac{n}{p^3}\right]\right) + \ldots \\ &= \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \ldots \end{aligned}$$

[13] Die Aussage, daß $\lim_{x \to \infty} \frac{\pi(x)}{x/\log x} = 1$ gilt ist einerseits stärker (für genügend große x können a und b beliebig nahe bei eins gewählt werden) als auch schwächer (weil nur asymptotische Aussagen getroffen werden).

2. Hier verwenden wir Induktion nach n. Für den Induktionsanfang $n < p$ ist die Behauptung klar.

   Induktionsschritt: $n \rightsquigarrow n+1$:

   Sei $n+1 = \sum_{i \geq s} a_i p^i, \quad a_s \neq 0$ die p-adische Entwicklung von $n+1$. Dann ist

   $n = p-1+(p-1)p+\ldots(p-1)p^{s-1}+(a_s-1)p^s+\sum_{i>s} a_i p^i$ und $l_p(n+1) = l_p(n) - s(p-1)+1$.

   Deshalb gilt: $v_p((n+1)!) = v_p(n!)+v_p(n+1) = v_p(n!)+s = \frac{n+1-l_p(n+1)}{p-1}$.

3. $\frac{n}{p}-1 < \left[\frac{n}{p}\right] \underset{(1.)}{\leq} v_p(n!) \underset{(2.)}{=} \frac{n-l_p}{p-1} \leq \frac{n-1}{p-1} < \frac{n}{p-1} = \frac{n}{p} + \frac{n}{p(p-1)}$

□

Korollar 8.2 (Teilbarkeit von Binomialkoeffizienten): Seien $n = \sum n_i p^i, k = \sum k_i p^i$ die p-adischen Entwicklungen von $n, k \in \mathbb{N}_0, p \in \mathbb{P}$. Mit der Konvention $\binom{a}{b} = 0$ falls $a < b$, gilt:

$$\begin{aligned}\binom{n}{k} \not\equiv 0 \pmod{p} &\Leftrightarrow \forall\, i \text{ ist } \binom{n_i}{k_i} \not\equiv 0 \pmod{p} \\ &\Leftrightarrow \forall\, i \text{ ist } k_i \leq n_i \\ &\Leftrightarrow \text{Die } p\text{-adischen Ziffern von } n \text{ sind die Summe der entsprechenden Ziffern von } k \text{ und von } n-k \\ &\quad \text{(”Es gibt keinen Übertrag bei der Entwicklung von } n = k+(n-k)\text{”)} \\ &\Leftrightarrow l_p(n) = l_p(k)+l_p(n-k)\end{aligned}$$

Beweis : Alle Äquivalenzen bis auf die erste sind klar, und für diese gilt:

$$\begin{aligned}\binom{n}{k} \not\equiv 0 \pmod{p} &\Leftrightarrow v_p\binom{n}{k} = 0 \\ &\Leftrightarrow v_p(n!) = v_p(k!)+v_p((n-k)!) \\ &\underset{(8.1,2)}{\Leftrightarrow} \frac{n-l_p(n)}{p-1} = \frac{k-l_p(k)}{p-1} + \frac{n-k+l_p(n-k)}{p-1} \\ &\Leftrightarrow l_p(n) = l_p(k)+l_p(n-k)\end{aligned}$$

□

Proposition 8.3 (Ungleichungen für Binomialkoeffizienten): Für $n \in \mathbb{N}$ und die Binomialkoeffizienten $\binom{*}{*}$ gelten:

$$2^n \leq \binom{2n}{n} < \binom{2n+1}{n} < 4^n < (2n+1)\binom{2n}{n} = (n+1)\binom{2n+1}{n}$$

Beweis : 1. Ungleichung: Wir verwenden Induktion nach n: $n = 1$ ist klar, und im Induktionsschritt vergrößert sich 2^n um den Faktor 2, und $\binom{2n}{n}$ um den Faktor $\frac{(2n+1)(2n+2)}{(n+1)^2} > 2$. Die vierte Ungleichung geht ebenfalls mittels Induktion, die zweite Ungleichung und die letzte Gleichung sind trivial. Für die dritte Ungleichung gilt:

$$4^n = \frac{1}{2}(1+1)^{2n+1} = \frac{1}{2}\sum_{0 \leq i \leq 2n+1}\binom{2n+1}{i} \overset{i=n,n+1}{>} \frac{1}{2}\binom{2n+1}{n} + \frac{1}{2}\underbrace{\binom{2n+1}{n+1}}_{=\binom{2n+1}{n}} = \binom{2n+1}{n}$$

Ab jetzt gelte bis zum Ende des Kapitels die Konvention: $p, q \in \mathbb{P}, \sum_{p \leq x} \cdot \hat{=} \sum_{\substack{p \leq x \\ p \in \mathbb{P}}} \cdot$.

Proposition 8.4 (Primzahlschranke): Für $n \in \mathbb{N}$ gilt: $\prod_{p \leq n} p < 4^n$.

Beweis : Für $n = 1,2$ ist die Aussage trivial. Für $n \geq 3$ verwenden wir Induktion: Induktionsschritt: $n-1 \rightsquigarrow n$:

$\underline{n \text{ gerade}}$: $\prod_{p \leq n} p = \prod_{p \leq n-1} p \underset{\text{Ind.Vor.}}{\leq} 4^{n-1} < 4^n$.

$\underline{n \text{ ungerade}}$, d.h. $n = 2m+1 :< \prod_{m+1<p\leq 2m+1} p | \binom{2m+1}{m} \underset{(8.3)}{<} 4^m$.

Also gilt: $\prod_{p \leq 2m+1} p = \prod_{p \leq m+1} p \prod_{m+1<p\leq 2m+1} p \overset{\text{I.V.}}{<} 4^{m+1}4^m = 4^{2m+1}$.

□

Satz 8.5 (Abschätzung des kgV): Sei $d_n := kgV\{1,2,\ldots n\}, n \in \mathbb{N}$. Dann ist für $n \geq 7$ immer $d_n > 2^n$, wie auch folgende Tabelle verdeutlicht:

n	2	3	4	5	6	7	8	9	10	11	12
2^n	4	8	16	32	64	128	256	512	1024	2048	4096
d_n	2	6	12	60	60	420	840	2520	2520	27720	27720

Beweis :

1. Wir berechnen das Integral $I(m,n) := \int_0^1 x^{m-1}(1-x)^{n-m}dx, \quad 1 \leq m \leq n, \quad m,n \in \mathbb{N}$, auf zwei verschiedene Arten:

   Wegen $(1-x)^{n-m} = \sum_{0\leq j\leq n-m} \binom{n-m}{j}(-1)^j x^j$ gilt:

   $$I(m,n) = \sum_{0\leq j\leq n-m} (-1)^j \binom{n-m}{j} \int_0^1 x^{m-1+j}dx = \sum_{0\leq j\leq n-m} (-1)^j \binom{n-m}{j} \frac{1}{m+j} \in \frac{1}{d_n}\mathbb{Z},$$

   denn d_n ist der Hauptnenner der Summanden.

2. Um das Integral auf die zweite Art zu berechnen, berechnen wir auch das folgende Integral auf zwei Arten. Dabei sei $y \in [0,1)$.

   $$\begin{aligned}\int_0^1 (1-x+xy)^{n-1}dx &= \sum_{0\leq m\leq n-1} \binom{n-1}{m} \int_0^1 (1-x)^{n-m-1}(xy)^m dx \\ &= \sum_{1\leq m\leq n} \binom{n-1}{m-1} \int_0^1 (1-x)^{n-m}(xy)^{m-1}dx \\ &= \sum_{1\leq m\leq n} \binom{n-1}{m-1} y^{m-1} I(m,n)\end{aligned}$$

3. $$\int_0^1 (1-x+xy)^{n-1} = \frac{(1-x+xy)^n}{x(y-1)}\Big|_{x=0}^{x=1} = \frac{y^n}{n(y-1)} - \frac{1}{n(y-1)} = \frac{1}{n}\left(\frac{y^n-1}{y-1}\right) = \frac{1}{n}(1+y+y^2+\ldots y^{n-1})$$

4. Wegen der linearen Unabhängigkeit der Faktoren $1, y, y^2, \ldots$ auf [0,1) können wir Koeffizientenvergleich anwenden und erhalten:

   $$\binom{n-1}{m-1} I(m,n) = \frac{1}{n}, \text{ d.h. } I(m,n) = \frac{1}{n\binom{n-1}{m-1}} = \frac{1}{m\binom{n}{m}} \quad \text{für } 1 \leq m \leq n$$

5. Ein Vergleich mit (1.) zeigt: $\exists\, c \in \mathbb{N}$ mit

   $$\frac{1}{m\binom{n}{m}} = \frac{c}{d_n}, \text{ d.h. } d_n = cm\binom{n}{m}, \text{ d.h. } m\binom{n}{m} \mid d_n$$

6. Insbesondere gelten: $n\binom{2n}{n} \mid d_{2n} \mid d_{n+1}$, und $(2n+1)\binom{2n}{n} = (n+1)\underbrace{\binom{2n+1}{n+1}}_{=\binom{2n+1}{n}} \mid d_{2n+1}$.

   Wegen (n,2n+1) = 1 ist auch $n\underbrace{(2n+1)\binom{2n}{n}}_{>4^n \text{ nach } (8.3)} \mid d_{2n+1}$, also gilt: $d_{2n+1} > n4^n$.

7. Folglich gilt $\begin{array}{rlll} \text{für } n \geq 2: & d_{2n+1} & > 2 \cdot 4^n & = 2^{2n+1} \\ \text{und für } n \geq 4: & d_{2n+2} & \geq d_{2n+1} \geq 4^{n+1} & = 2^{2n+2} \end{array}$ was die Behauptung zeigt für ungerade $n \geq 5$ und gerade $n \geq 10$. Den Fall $n = 8$ haben wir für die Tabelle schon nachgerechnet.

□

Die letzte Aussage und ihr Beweis stammen von M.Nair (Journal London Mathematical Society, 1982).

Satz 8.6 (Abschätzung der Primzahlfunktion): Für alle $n \in \mathbb{N}, n \geq 4$ gelten die Ungleichungen:

$$\log 2 \frac{n}{\log n} \leq \pi(n) \leq \left(\log 4 + 8\frac{\log\log n}{\log n}\right)\frac{n}{\log n}$$

Anmerkung: $\log 2 = 0.6931\ldots$, $\log 4 = 1.386\ldots$

Beweis : Erste Ungleichung: Sei p ein Primteiler von d_n, $p^e \| d_n, e \in \mathbb{N}$. Es existiert ein $m \leq n$ mit $p^e \| m$. Deshalb gilt:

$$d_n = \prod_{\substack{p \leq n \\ p^e \| d_n}} p^e \leq \prod_{p \leq n} n = n^{\pi(n)}$$

$$\rightsquigarrow \log d_n \leq \pi(n) \log n$$

$$\rightsquigarrow \pi(n) \overset{(8.5), n \geq 7}{\geq} \frac{\log 2 \cdot n}{\log n}$$

Die Fälle $n = 4, 5, 6$ gelten ebenfalls, wie man durch Nachrechnen bestätigt.

Zweite Ungleichung:

1. Sei $t \in [1, n]$. Es ist

$$\begin{aligned} & t^{\pi(n)-\pi(t)} \prod_{t < p \leq n} p \underset{(8.4)}{\leq} 4^n \\ \rightsquigarrow & (\pi(n) - \pi(t)) \log t \leq n \log 4 \\ \rightsquigarrow & \pi(n) \leq \frac{n \log 4}{\log t} + \pi(t) \leq \frac{n \log 4}{\log t} + t \end{aligned}$$

2. Als Funktion in t hat $\frac{n\log 4}{\log t} + t$ ein Minimum bei t mit $n \log 4 = t(\log t)^2$ (← nicht elementar auflösbar nach t).

   Wähle stattdessen $t := \frac{n}{(\log n)^2}$. Dies liefert $\pi(n) \leq \frac{n\log 4}{\log n - 2\log\log n} + \frac{n}{(\log n)^2} = \frac{n}{\log n}\left(\frac{\log 4}{1 - \frac{2\log\log n}{\log n}} + \frac{1}{\log n}\right)$

   Die behauptete Ungleichung folgt nun aus:

$$\log 4 + 8\frac{\log\log n}{\log n} \geq \frac{\log 4}{1 - \frac{2\log\log n}{\log n}} + \frac{1}{\log n}.$$

   Wegen $\lim_{x\to\infty} \frac{\log\log n}{\log n} = 0$ ist einleuchtend, daß diese gelten wird für genügend große n. Eine entsprechende Schranke werden wir im folgenden finden. Für die kleineren n vergleicht man dann $\pi(x)$ direkt mit $\log 4 + 8\frac{\log\log n}{\log n}$.

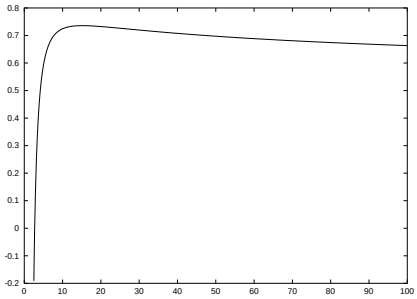


Abbildung 3: Das Bild von L. Wie im Text gezeigt hat L eine Nullstelle bei $x = e$, einen Hochpunkt bei $x = e^e$ und geht gegen 0 für $x \to \infty$.

3. Setze $L = L(x) = 2\frac{\log\log x}{\log x}$. Es ist $L(x) > 0 \overset{x>1}{\Leftrightarrow} \log\log x > 0 \Leftrightarrow \log x > 1 \Leftrightarrow x > e$.

   Ab jetzt sei immer $x > e$. Weiter ist $L'(x) = 2\frac{1-\log\log x}{x(\log x)^2}$ und es gilt: $L'(x) = 0 \Leftrightarrow \log\log x = 1 \Leftrightarrow x = e^e \approx 15{,}15\ldots$

   Beachte: Ab $x = e^e$ ist $L(x)$ monoton fallend, $L(e^e) = \frac{2}{e} < 1$ (vgl. Bild).

4. $$\begin{aligned}
   &\log 4 + 8\frac{\log\log n}{\log n} \geq \frac{\log 4}{1 - \frac{2\log\log n}{\log n}} + \frac{1}{\log n} \\
   \Leftrightarrow &\frac{\log 4}{1-L} + \frac{1}{\log n} \leq \log 4 + 4L \\
   \Leftrightarrow &\log 4\left(\frac{1}{1-L} - 1\right) \leq 4L - \frac{1}{\log n} \\
   \Leftrightarrow &\frac{\log 4}{4}\left(\frac{L}{1-L}\right) \leq L - \frac{1}{4\log n} \\
   \overset{L,1-L>0}{\Leftrightarrow} &\frac{\log 4}{4} \leq 1 - L - \frac{1-L}{4L\log n} \\
   \Leftrightarrow &L \leq 1 - \frac{\log 2}{2} - \frac{1}{8\log\log n} + \frac{1}{4\log n} \quad (*)
   \end{aligned}$$

5. Wir betrachten beide Seiten von $(*)$ als Funktion in x. Die Ableitung der rechten Seite ist:

   $$\frac{1}{8x\log x(\log\log x)^2} - \frac{1}{4x(\log x)^2} = \frac{1}{4x\log x}\left(\frac{1}{2(\log\log x)^2} - \frac{1}{\log x}\right).$$

6. $$\begin{aligned}
   &\text{Ableitung der linken Seite } < \text{ Ableitung der rechten Seite} \\
   \Leftrightarrow &\frac{2(1-\log\log x)}{x(\log x)^2} < \frac{1}{4x\log x}\left(\frac{1}{2(\log\log x)^2} - \frac{1}{\log x}\right) \\
   \Leftrightarrow &\frac{8}{\log x}(1-\log\log x) < \left(\frac{1}{2(\log\log x)^2} - \frac{1}{\log x}\right) \\
   \Leftrightarrow &9 < 8\log\log x + \frac{\log x}{2(\log\log x)^2} \leftarrow \text{ monoton steigend für } x > e^e.
   \end{aligned}$$

   Weil diese Ungleichung erfüllt ist für $x = e^e$, ist sie deshalb auch erfüllt für $x \geq e^e$.

7. Also gilt: Ist $(*)$ erfüllt für ein $x_0 > e^e$, so ist $(*)$ schon für alle $x \geq x_0$ erfüllt.

8. Setze $x_0 = 250$. Dann ist $L(x_0) = 0.618\ldots$ und die rechte Seite von $(*)$ wird zu $0.625\ldots$, wenn x_0 eingesetzt wird. Deshalb sind die Bedingungen aus (7) erfüllt.

9. Für die $n \in \mathbb{N}$ mit $4 \leq n < 250$ zeigt man die behauptete Ungleichung direkt.

□

Korollar 8.7 (Abschätzung der Primzahlfunktion): $\underline{\lim}_{x\to\infty} \frac{\pi(x)}{x/\log x} \geq \log 2$, $\overline{\lim}_{x\to\infty} \frac{\pi(x)}{x/\log x} \leq \log 4$

□

Bemerkung 8.8 (Primzahlschranken von Tschebyschew): Zwischen 1850 und 1860 hat Tschebyschew mehrere Ungleichungen der Form

$$(a+f(x))\frac{x}{\log x} \leq \pi(x) \leq (b+g(x))\frac{x}{\log x}, \quad \text{für } y \geq c$$

gezeigt, wobei $f(x), g(x)$ gegen 0 gehen für x gegen unendlich.

Beispiel: $a = \log(2^{1/2}\cdot 3^{1/3}\cdot 5^{1/5}\cdot 30^{-1/30}) = 0.9219\ldots$, $b = \frac{6}{5}a = 1.1055\ldots$, $f,g = 0$, mit großem c.

Eine der besten verfügbaren expliziten Abschätzungen ist wie folgt:

$$\left(1+\frac{1}{2\log x}\right)\frac{x}{\log x} \leq \pi(x) \leq \left(1+\frac{3}{2\log x}\right)\frac{x}{\log x}, \quad x \geq 52.$$

Die Funktion $\frac{x}{\log x}$ ist eine sehr schlechte Approximation für $\pi(x)$. In Wirklichkeit ist $\pi(x) > \frac{x}{\log x}$ für $x \geq 52$. Eine bessere Approximation von $\pi(x)$ ist

$$li(x) = \int_2^x \frac{dt}{\log t}.$$

Die folgende Tabelle verdeutlicht dies:

x	$\pi(x)$	$\frac{x}{\log x}$	$li(x)$
10	4	$4,3\ldots$	$5,12\ldots$
10^2	25	$21,7\ldots$	$29,08\ldots$
10^3	168	$144,7\ldots$	$176,56\ldots$
10^4	1229	$1085,7\ldots$	$1245,09\ldots$
10^7	664.578	$620.420,7\ldots$	$664.918,\ldots$
10^{10}	455.052.511	$\approx 4,34\cdot 10^8$	$\approx 4,55056\cdot 10^8$

Momentan (23.06.2003) ist der genaue Wert von $\pi(x)$ bekannt für $x = 10^{22}$.

Akzeptiert man $li(x)$ als Approximation für $\pi(x)$, dann gilt:

$$P(n \approx x, n \in \mathbb{P}) = \frac{\#\{p \in \mathbb{P} | x-k \leq p \leq x+k\}}{\#\{n \in \mathbb{N} | x-k \leq n \leq x+k\}} \approx \frac{d}{dx} li(x)\Big|_x = \frac{1}{\log x}.$$

Dabei ist k klein gegenüber n, aber groß genug, um zufällige Schwankungen auszumitteln. Weiter gilt: Akzeptiert man $\pi(n) \approx \frac{n}{\log n}$, dann kann man die "Umkehrfunktion" $n \mapsto p_n$ abschätzen durch $n\log n$. Eine bessere Approximation ist $p_n \approx n(\log n + \log\log n - 1)$. Es ist sogar bewiesen, daß für alle $n > 8601$ gilt:

$$n(\log n + \log\log n - 1.0073) < p_n < n(\log n + \log\log n - 0.9385).$$

Beispielsweise ergibt sich für $n = 10.000$ die Ungleichung $104.234 < p_n < 104.922$.

Exakt ist $p_{10.000} = 104.719$.

9 Weitere Sätze über Primzahlen

In diesem Kapitel wollen wir die Summe $\sum_{p\leq x} \frac{1}{p}$ und das Produkt $\prod_{p\leq x}\left(1-\frac{1}{p}\right)$ berechnen. Dazu betrachten wir zuerst die folgende Definition:

Definition 9.1 (Asymptotische Äquivalenz): Seien f,g Funktionen auf einer Teilmenge D von $\mathbb{R}$. Wir schreiben

1. $f \sim g :\Leftrightarrow \lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$. Dies gibt nur Sinn, falls D nach oben unbeschränkt ist. Diese Äquivalenzrelation heißt **asymptotische Äquivalenz**. So gilt beispielsweise $\pi(x) \sim \frac{x}{\log x}$.
2. $f = o(g) :\Leftrightarrow \lim_{x\to\infty} \frac{f(x)}{g(x)} = 0$. Auch dies macht nur Sinn, falls D nach oben unbeschränkt ist.
3. $f = O(g) :\Leftrightarrow \exists\, c > 0\ \forall\, x \in D : |f(x) \leq c|g(x)|$.

Satz 9.2 (Satz von Mertens): Es gilt: $\sum_{p\le x}\frac{\log p}{p}=\log x+R_x,\quad R_x\in(-1-\log 4,\log 4)$.

Insbesondere gilt $\sum_{p\le x}\frac{\log p}{p}-\log x=O(1)$, mit der Konstanten $c=1+\log 4$ in der O-Notation.

Beweis :

1. Sei $x>1, n:=[x]$. Wir wissen aus 6.7: $\log(n!)=n\log n-n+1+\theta_n\log n$ mit $\theta_n\in[0,1]$.
2. $$\log n!=\sum_{p\le n}v_p(n!)\log p,\quad \frac{n}{p}-1<v_p(n!)<\frac{n}{p}+\frac{n}{p(p-1)}\ \text{(vgl. 8.1)}$$
$$\rightsquigarrow n\sum_{p\le n}\frac{\log p}{p}-\underbrace{\sum_{p\le n}\log p}_{\le n\log 4\ \text{nach 8.4}}<\log n!<n\sum_{p\le n}\frac{\log p}{p}+\sum_{p\le n}\frac{\log p}{p(p-1)}$$
3. $$n\sum_{p\le n}\frac{\log p}{p}-n\log 4<n\log n-n+1+\log n<n\log n,$$
d.h. $\sum_{p\le n}\frac{\log p}{p}<\log n+\log 4\le\log x+\log 4$(← erste behauptete Ungleichung).
Für die zweite Ungleichung gilt:
4. $$\sum_{p\in\mathbb{P}}\frac{\log p}{p(p-1)}<\sum_{2\le m}\frac{\log m}{m(m-1)}\le\sum_{r\ge 1}\sum_{2^{r-1}<m\le 2^r}\frac{r\log 2}{m(m-1)}=\sum_{r\ge 1}r\log 2\underbrace{\sum_{2^{r-1}<m\le 2^r}\frac{1}{m(m-1)}}_{2^{-r}}$$
$$=\log 2\underbrace{\sum_{r\ge 1}\frac{r}{2^r}}_{=2}=2\log 2=\log 4$$
5. Deshalb folgt mit 2.:
$$n\sum_{p\le n}\frac{\log p}{p}+n\log 4\overset{1.,4.}{>}n\log n-n+1$$
$$\rightsquigarrow\sum_{p\le n}\frac{\log p}{p}>\log n+\frac{1}{n}-(1+\log 4)\ge\log x-(1+\log 4)$$

Noch offen sind die folgenden Punkte:

- $$\sum_{2^{r-1}<m\le 2^r}\frac{1}{m(m-1)}=2^{-r}$$
- $$\sum_{r\ge 1}\frac{r}{2^r}=2$$

Diese folgen aus den beiden folgenden Propositionen, die in den Übungen gezeigt wurden:

Proposition 9.3 (Unendliche Summe eines Bruchs): Es gilt:

$$S_k:=\sum_{m>k}\frac{1}{m(m-1)}=\frac{1}{k}.$$

(Vgl. Aufgabe 1, Blatt 9)

Proposition 9.4 (Potenzreihenidentität): Es gilt:

$$\sum_{r\geq 1} rX^r = \frac{X}{(1-X)^2}.$$

(Vgl. Aufgabe 4, Blatt 6)

Proposition 9.5 (Eine Summe über die Primzahlen): Die Summe

$$\sum_{p\in\mathbb{P}} \left(\log\left(\frac{1}{1-p^{-1}}\right) - \frac{1}{p}\right)$$

konvergiert absolut. Sei c_0 ihr Wert. ($c_0 = 0.315718\ldots$)

Beweis : Die Summe läßt sich umschreiben zu:

$$\sum_{p\in\mathbb{P}} \left(\sum_{k\geq 1} \frac{1}{kp^k} - \frac{1}{p}\right) = \sum_{p} \left(\sum_{k\geq 2} \frac{1}{kp^k}\right) = \sum_{p^k, k\geq 2} \frac{1}{kp^k} \leq \sum_{p}\sum_{k\geq 1} \frac{1}{p^{2l}} \leq \sum_{n\in\mathbb{N}} \frac{1}{n^2} < \infty$$

Dabei haben wir die Ungleichung

$$\frac{1}{2lp^{2l}} + \frac{1}{(2l+1)p^{2l+1}} \leq \frac{1}{p^{2l}}$$

verwendet.

□

Satz 9.6 (Summe über p^{-1}): Mit c_0 wie in (9.5) gilt:

$$(*) \quad \sum_{p\leq x} \frac{1}{p} = \log\left(\frac{1}{\prod_{p\leq x}\left(1-\frac{1}{p}\right)}\right) - c_0 + \frac{\theta_x}{2(x-1)} \quad (\theta_x \in (0,1)).$$

Mit anderen Worten:

$$\sum_{p\leq x} \frac{1}{p} - \log\left(\frac{1}{\prod_{p\leq x}\left(1-\frac{1}{p}\right)}\right) + c_0 = O\left(\frac{1}{x-1}\right) = O\left(\frac{1}{x}\right) \quad \text{für } x \geq 2.$$

Beweis : Einsetzen von c_0 und auflösen nach θ_x in (*) liefert:

$$\theta_x = 2(x-1)\sum_{p\geq x}\left(\log\left(\frac{1}{1-p^{-1}}\right) - \frac{1}{p}\right) (\leftarrow \text{ lauter Terme} \geq 0, \text{ also ist } \theta_x \geq 0)$$

$$= 2(x-1)\sum_{p\geq x}\sum_{k\geq 2}\frac{p^{-k}}{k} < \sum_{p>x}\frac{2(x-1)}{2p(p-1)} < \sum_{n>x}\frac{x-1}{n(n-1)} \overset{(9.3)}{=} \frac{x-1}{N-1} < 1$$

Dabei ist N die kleinste natürliche Zahl $> x$. Für die vorletzte Ungleichung haben wir folgendes verwendet (mit $t := p^{-1}$):

$$\sum_{k\geq 2}\frac{t^k}{k} < \frac{1}{2}\sum_{k\geq 2} t^k = \frac{1}{2}\frac{t^2}{1-t} = \frac{1}{2t^{-1}(t^{-1}-1)},$$

wobei $0 \leq t < 1$.

□

Satz 9.7 (Summe über Inverse der Primzahlen): Es existiert eine Konstante $c_1 \in \mathbb{R}$, so daß für alle $x \geq 2$ gilt:

$$\sum_{p\leq x}\frac{1}{p} = \log\log x + c_1 + O\left(\frac{1}{\log x}\right).$$

Die Konstante c zum O-Symbol kann kleiner als $2(1+\log 4) < 5$ gewählt werden.

Beweis :

$$R(t) := \sum_{p\le x}\frac{\log p}{p} - \log(t) \quad (= O(1) \text{ nach 9.2})$$

$$\begin{aligned}
\sum_{p\le x}\frac{1}{p} &= \int_{2-}^{x}\frac{1}{\log t}d\left(\sum_{p\le t}\frac{\log p}{p}\right)(t) = \int_{2-}^{x}\frac{1}{\log t}d\log t + \int_{2-}^{x}\frac{1}{\log t}dR(t)\\
&= \int_{2-}^{x}\frac{1}{\log t}\frac{1}{t}dt + \int_{2-}^{x}\frac{1}{\log t}dR(t) = \int_{2}^{x}\underbrace{\frac{1}{\log t}\frac{1}{t}}_{(\log\log t)'}dt + \int_{2-}^{x}\frac{1}{\log t}dR(t)\\
&= \log\log x - \log\log 2 + \frac{R(t)}{\log t}\Big|_{2-}^{x} - \int_{2-}^{x}R(t)d\left(\frac{1}{\log t}\right)\\
&= \log\log x - \log\log 2 + \frac{R(x)}{\log x} - \underbrace{\frac{R(2-)}{\log 2}}_{=-1} + \int_{2-}^{x}\frac{R(t)}{t(\log t)^2}dt.
\end{aligned}$$

Wir setzen $R := \sup_{t\ge 2-}|R(t)| \overset{9.2}{\le} 1+\log 4$. Dann gilt:

$$\left|\frac{R(t)}{\log x} - \underbrace{\int_x^\infty \frac{R(t)}{t(\log t)^2}dt}_{\le R\int_x^\infty \frac{dt}{t(\log t)^2} = R\left|\frac{1}{\log t}\right|_x^\infty = \frac{R}{\log x}}\right| \le 2\frac{R}{\log x}$$

und deshalb

$$\sum_{p\le x}\frac{1}{p} - \log\log x = \underbrace{\frac{R(x)}{\log x} - \int_x^\infty \frac{R(t)dt}{t(\log t)^2}}_{O\left(\frac{1}{\log x}\right)} + \underbrace{\int_{2-}^\infty \frac{R(t)dt}{t(\log t)^2} - \log\log 2 + 1}_{=:c_1,\ \text{unabhängig von } x}.$$

□

Korollar 9.8 (Produkt über $1-\frac{1}{p}$): Mit den Konstanten c_0 und c_1 wie in (9.5) bzw. (9.7) gilt:

$$\prod_{p\le x}\left(1-\frac{1}{p}\right) = \frac{e^{-(c_0+c_1)}}{\log x}\left(1+O\left(\frac{1}{\log x}\right)\right)$$

Beweis :

$$\begin{aligned}
\prod_{p\le x}\left(1-\frac{1}{p}\right) &= e^{-\log\left(\prod_{p\le x}(1-\frac{1}{p})^{-1}\right)} \overset{9.6}{=} e^{-\sum_{p\le x}\frac{1}{p} - c_0 + \frac{\theta_x}{2(x-1)}} \quad \theta_x\in(0,1)\\
&\overset{9.7}{=} e^{-\log\log x - c_1 + O(\frac{1}{\log x}) - c_0 + \frac{\theta_x}{2(x-1)}} = \frac{e^{-(c_0+c_1)+O(\frac{1}{\log x})}}{\log x}\\
&= \frac{e^{-(c_0+c_1)}}{\log x}e^{O(\frac{1}{\log x})}\\
&= \frac{e^{-(c_0+c_1)}}{\log x}\left(1+O\left(\frac{1}{\log x}\right)\right), \text{ da } |e^h-1|\le \text{ const.}\cdot h, \text{ falls } h\in[0,1]
\end{aligned}$$

□

Satz 9.9 (Formel von Mertens): Es gilt: $c_0+c_1=\gamma$. Dabei ist γ die Euler-Konstante aus (6.10). Insbesondere gilt:

$$\prod_{p\le x}\left(1-\frac{1}{p}\right) = \frac{e^{-\gamma}}{\log x}\left(1+O\left(\frac{1}{\log x}\right)\right)$$

Beweis :

1. $\zeta(s) = \sum_{n\geq 1} n^{-s} = \prod_{p\in\mathbb{P}} \left(1-\frac{1}{p^s}\right)^{-1} \quad (s\in\mathbb{R}, s>1).$

   Wir betrachten das Verhalten bei $s \to 0+$ von:

$$\begin{aligned} f(s) &:= \log\zeta(1+s) - \sum_{p\in\mathbb{P}} p^{-1-s} \quad (s\in\mathbb{R}, 0<0\leq 1) \\ &= \sum_{p\in\mathbb{P}} \log\left(\frac{1}{1-p^{-1-s}}\right) - \sum_{p\in\mathbb{P}} p^{-1-s} \\ &= \sum_{p\in\mathbb{P}}\sum_{k\geq 1} \frac{p^{-k(1+s)}}{k} - \sum_{p\in\mathbb{P}} p^{-1-s} \\ &= \sum_{p\in\mathbb{P}}\sum_{k\geq 2} \frac{p^{-k(1+s)}}{k} \\ &\leq \sum_{\substack{p\in\mathbb{P}\\ k\geq 2}} \frac{p^{-k}}{k} \quad \text{(Die Summe ist absolut konvergent für } s\geq 0 \text{ und es gilt: } f(0)=c_0.) \end{aligned}$$

   D.h. das “Hindernis” für die Konvergenz von $\sum_{n\geq 1} n^{-s}$ an $s=1$ ist die Teilsumme $\sum_{p\in\mathbb{P}} n^{-s}$.

2. Für $0<s\leq 1$ gilt:

$$\begin{aligned} \zeta(1+s) = \sum_{n\geq 1} n^{-(1+s)} &\overset{(6.7)}{=} \int_1^\infty x^{-1-s}dx + 1 + \theta(-1) \quad \theta\in[0,1] \\ &= -\frac{x^{-s}}{s}\Big|_{x=1}^{x=\infty} + O(1) = \frac{1}{s} + \underbrace{O(1)}_{\text{unabhängig von } s} = \frac{1}{s}(1+O(s)). \end{aligned}$$

3. Deshalb

$$\begin{aligned} \log\zeta(1+s) &= \log\left(\frac{1}{s}(1+O(s))\right) = \log\left(\frac{1}{s}\right) + \underbrace{\log(1+O(s))}_{O(s)} \\ &= \underbrace{\log\left(\frac{1}{1-e^{-s}}\right)}_{=\log\frac{1}{s}+O(s)} + O(s) = \sum_{n\geq 1}\frac{e^{-sn}}{n} + O(s) \\ &= \int_0^\infty e^{-st}dH(t) + O(s) \overset{\text{part. Int.}}{=} \underbrace{e^{-st}H(t)\big|_{t=0}^{t=\infty}}_{=0} - \int_0^\infty H(t)d(e^{-st}) + O(s) \\ &= s\int_0^\infty H(t)e^{-st}dt + O(s) \qquad \text{mit } H(t) := \sum_{n\in\mathbb{N}1\leq n\leq t}\frac{1}{n} \text{vgl. (6.10)} \end{aligned}$$

4. Sei $P(n) := \sum_{p\leq n}\frac{1}{p}$. Dann gilt:

$$\sum_{p\in\mathbb{P}} p^{-1-s} = \int_1^\infty u^{-s}dP(u) \overset{\text{part.Int}}{=} s\int_1^\infty P(u)u^{-1-s}du \overset{u:=e^t=\frac{du}{dt}}{=} s\int_0^\infty e^{-st}P(e^t)dt.$$

5. Es ist

$$H(t) = \log t + \gamma + O\left(\frac{1}{t}\right) \qquad (\text{ nach } (6.10))$$

$$P(e^t) = \sum_{p \le e^t} \frac{1}{p} \overset{(9.7)}{=} \log\log e^t + c_1 + O\left(\frac{1}{\log e^t}\right) = \log t + c_1 + O\left(\frac{1}{t}\right)$$

$$\rightsquigarrow H(t) - P(e^t) = \gamma - c_1 + O\left(\frac{1}{t}\right) \quad (t \ge 1)$$

$$= \gamma - c_1 + O\left(\frac{1}{t+1}\right) \quad (t \ge 0)$$

$$f(s) \overset{(i) \text{ bis } (iv)}{=} s\int_0^\infty e^{-st}(H(t) - P(e^t))dt + O(s)$$

$$= s\int_0^\infty e^{-st}(\gamma - c_1)dt + s\int_0^\infty e^{-st}\left(O\left(\frac{1}{t+1}\right)\right)dt + O(s)$$

$$= \gamma - c_1 + O\left(s\int_0^\infty \frac{e^{-st}}{t+1}dt\right) + O(s)$$

6. Weiter ist

$$\int_0^\infty \frac{e^{-st}}{t+1}dt = \sum_{k\ge1}\frac{e^{-sk}}{k+1} + \theta\left.\frac{e^{-st}}{t+1}\right|_{t=0} \qquad \theta \in [0,1]$$

$$= \sum_{k\ge0}\frac{e^{-sk}}{k+1} + O(1) = e^s\sum_{k\ge1}\frac{e^{-sk}}{k} + O(1) = e^s\log\underbrace{\frac{1}{1-e^{-s}}}_{O(s)} + O(1)$$

$$= e^s O(\log(s^{-1})) + O(1) = O(\log s^{-1})$$

7. Zusammen also $f(s) = \gamma - c_1 + O(sO(\log s^{-1})) + O(s) = \gamma - c_1 + O(s\log s^{-1}) + O(s)$.
   Weiter gilt: $c_0 \overset{1.}{=} \lim_{s\to0} f(s) = \gamma - c_1 + \underbrace{\lim_{s\to0} O(s\log s^{-1})}_{=0 \text{ (Regel von de l'Hôpital)}} = \gamma - c_1$

□

Schlußbemerkungen: Die Konstanten γ und c_0 sind relativ leicht zu approximieren. Mit ihrer Hilfe kann man deshalb auch c_1 näherungsweise bestimmen: $c_1 = \gamma - c_0 \approx 0.26149\ldots$.

In (9.7) haben wir gezeigt: $\sum_p \frac{1}{p} = \log\log x + c_1 + O\left(\frac{1}{\log x}\right)$. Inbesondere geht die Summe der reziproken Primzahlen also gegen unendlich. Nimmt man aber alle zur Zeit "bekannten" Primzahlen (momentan sind alle Primzahlen kleiner 10^{22} "bekannt"[14]) und wertet die Summe aus, ist man noch sehr weit von unendlich entfernt, wie folgende Rechnung zeigt:

$$\sum_{p\le10^{22}}\frac{1}{p} \overset{9.7}{\le} \log\log 10^{22} + 0.26149\ldots + 2(1+\log 4)\left(\frac{1}{\log 10^{22}}\right) \approx 4.3 \ll \infty.$$

10 Arithmetische Funktionen und Dirichlet-Reihen

Definition 10.1 (Arithmetische Funktion): Eine arithmetische Funktion ist eine Abbildung $f : \mathbb{N} \to \mathbb{C}$.

Eine arithmetische Funktion f heißt (**schwach**) **additiv** $:\Leftrightarrow f(mn) = f(m) + f(n)$ falls $(m,n) = 1$
multiplikativ $:\Leftrightarrow f(mn) = f(m)\cdot f(n)$ falls $(m,n) = 1$.

f heißt **vollständig** **additiv** $:\Leftrightarrow f(mn) = f(m) + f(n) \quad \forall\,(m,n) \in \mathbb{N}^2$
multiplikativ $:\Leftrightarrow f(mn) = f(m)\cdot f(n) \quad \forall\,(m,n) \in \mathbb{N}^2$.

Ist $f\left\{\begin{array}{c}\text{additiv}\\ \text{multiplikativ}\end{array}\right\}$, so gilt bei bekannter Primfaktorzerlegung $n = \prod p_i^{e_i}$: $f(n) = \left\{\begin{array}{c}\sum f(p_i^{e_i})\\ \prod f(p_i^{e_i})\end{array}\right\}$.

[14] Genauer gesagt, ist der Wert die π-Funktion für diesen Wert bekannt.

Beispiele/Definitionen 10.2 (Möbius-Funktion):

1. Die Eulersche φ-Funktion ist multiplikativ.

2. $$\omega : \mathbb{N} \to \mathbb{N}_0 : \omega(n) := \#\{p \in \mathbb{P} |\ p | \ n\} \qquad \text{ist additiv.}$$
   $$\Omega(n) : \mathbb{N} \to \mathbb{N}_0 : \Omega(n) := \#\{p^{e_i} |\ p \in \mathbb{P}, e_i \in \mathbb{N}, p^{e_i} | n\} \qquad \text{ist vollständig additiv.}$$

   Mit der Primfaktorzerlegung $n = \prod p_i^{e_i}$ gilt: $\Omega(n) = \sum e_i$.

3. Für $k \in \mathbb{N}_0$ sei σ_k definiert durch
   $$\sigma_k(n) := \sum_{\substack{d \in \mathbb{N} \\ d | \ n}} d^k.$$

   Speziell sei $\tau(n) := \sigma_0(n) = \#\{d | \ n\}$, $\sigma(n) := \sigma_1(n)$.

   Alle σ_k sind multiplikativ. (Leichte Übung)

4. $$\mu : \mathbb{N}_0 \to \{\pm 1, 0\}$$
   $$n \mapsto \left\{ \begin{array}{cc} (-1)^{\omega(n)} & n \text{ quadratfrei} \\ 0 & \text{sonst} \end{array} \right\} \text{ ist multiplikativ.}$$

   Es gilt:
   $$\mu(p^e) = \left\{ \begin{array}{ll} 1 & e = 0 \\ -1 & e = 1 \\ 0 & e \geq 2 \end{array} \right. \qquad p \in \mathbb{P}, e \in \mathbb{N}_0 .$$

Proposition 10.3 (Summe über $\mu(d)$): Es gilt:
$$\sum_{d | \ n} \mu(d) = \left\{ \begin{array}{ll} 1 & n = 1 \\ 0 & n \neq 1 \end{array} \right.$$

Beweis : Wir verwenden Induktion über $\omega(n)$:

$\omega(n) = 0 \Leftrightarrow n = 1$ ist klar.

$\omega(n) = 1 \Rightarrow n = p^e$: $\quad \sum_{d | \ n} \mu(d) = \underbrace{\mu(1)}_{1} + \underbrace{\mu(p)}_{-1} + \underbrace{\mu(p^2)}_{0} + \ldots.$

$\omega(n) > 1$, d.h. $n = p^e m$, mit $p \in \mathbb{P}, e \geq 1$:

$$\sum_{d | \ n} \mu(d) = \sum_{d' | \ p^e} \sum_{d'' | \ m} \mu(d'd'') = \sum_{d' | \ p^e} \sum_{d'' | \ m} \mu(d')\mu(d'') = \left(\sum_{d' | \ p^e} \mu(d') \right) \left(\sum_{d'' | \ m} \mu(d'') \right) \overset{I.V.}{=} 0 \cdot 0 = 0$$

□

Satz 10.4 (Möbius-Inversion I): Sind f, g zwei arithmetische Funktionen, so sind äquivalent:

1. $g(n) = \sum_{d | \ n} f(d) \quad \forall\, n \in \mathbb{N}$
2. $f(n) = \sum_{d | \ n} \mu(\frac{n}{d}) g(d) \quad \forall\, n \in \mathbb{N}$

(Der Zusammenhang zwischen f und g ist analog zum Zusammenhang zwischen einer Funktion f und ihrer Fouriertransformierten $\hat{f}$.)

Beweis : Sei (1.) erfüllt. Dann gilt:

$$\sum_{d|\,n}\mu\left(\frac{n}{d}\right)g(d)=\sum_{d|\,n}\mu\left(\frac{n}{d}\right)\sum_{d'|\,d}f(d')=\sum_{d'|\,n}\underbrace{\sum_{d''|\,\frac{n}{d'}}\mu(d'')}_{\left\{\begin{array}{ll}0 & d'<n\\ 1 & d'=n\end{array}\right\}}f(d')=f(n).$$

Die zweite Implikation ergibt sich analog.

□

Satz 10.5 (Möbius-Inversion II): Seien F,G Funktionen auf $\mathbb{R}_{\geq 1}$, trivial fortgesetzt auf $\mathbb{R}_{\geq 0}$[15]. Dann sind äquivalent:

1. $G(x)=\sum_{n\leq x}F(\frac{x}{n})$
2. $F(x)=\sum_{n\leq x}\mu(n)G(\frac{x}{n})$

Beweis : Wir zeigen nur $(1.)\Rightarrow(2.)$, die zweite Implikation folgt analog:

$$\sum_{n\leq x}\mu(n)G\left(\frac{x}{n}\right)=\sum_{n\leq x}\mu(n)\sum_{m\leq\frac{x}{n}}F\left(\frac{x}{nm}\right)=\sum_{k\leq x}\sum_{\substack{m,n\\ mn=k}}\mu(n)F\left(\frac{x}{k}\right)$$

$$=\sum_{k\leq x}F\left(\frac{x}{k}\right)\underbrace{\left(\sum_{n|\,k}\mu(n)\right)}_{=\left\{\begin{array}{ll}0 & k>1\\ 1 & k=1\end{array}\right\}\text{ nach (10.3)}}=F(x)$$

□

Bemerkung 10.6 (Möbius-Inversion in abelschen Gruppen):

Aussage (10.4) bleibt richtig, falls $f,g:\mathbb{N}\to A$ Abbildungen mit Werten in einer abelschen Gruppe $(A,+)$ sind.

Beispiel 10.7 (primitive Einheitswurzeln): Frage: Wie viele primitive n-te Einheitswurzeln ζ gibt es in $\mathbb{C}$? Sei $\lambda(n):=\#\{\zeta\in\mathbb{C}|\zeta^n=1,\zeta^m\neq 1\forall\, m<n\}=\#\{\zeta\in\mathbb{C}|\zeta \text{ ist primitive } n\text{-te Einheitswurzel }\}$.

Es gilt:

$$\sum_{d|\,n}\lambda(d)=n\overset{2.20}{=}\sum_{d|\,n}\varphi(d).$$

Wende nun (10.4) an mit $g(n)=n, f(n)=\lambda(n)$(bzw. $\varphi(n)$). Also muß gelten: $\lambda=\varphi$. Es gibt also genau $\varphi(n)$ primitive n-te Einheitswurzeln.

Sei nun weiter

$$f_n(X)=\prod_{\substack{\zeta \text{ primitive}\\ n\text{-te Einheitswurzel}}}(X-\zeta)\quad\in\mathbb{C}[X]$$

und

$$g_n(X)=\prod_{\substack{\zeta\in\mathbb{C}\\ \zeta^n=1}}(X-\zeta)=X^n-1.$$

Dann gilt in $\mathbb{C}[X]$: $f_n|\ g_n$. Betrachte die Abbildungen $n\mapsto f_n(X)$ und $n\mapsto g_n(X)$, die beide von $\mathbb{N}$ in die multiplikative Gruppe $\mathbb{C}[X]^*$ des Körpers $\mathbb{C}[x]$ der rationalen Funktionen gehen (!). Es gilt: $g_n=\prod_{d|\,n}f_d(X)$. Wir wenden die Möbius-Inversion an und erhalten (dabei ist $\mathbb{C}[X]^*$ eine multiplikative Gruppe):

$$f_n(X)=\prod_{d|\,n}g_d(X)^{\mu(\frac{n}{d})}$$

[15] D.h. $F(x)$ und $G(x)$ sind 0 für $0\leq x<1$.

Beispielsweise gilt: $f_6(X) = \frac{(X^6-1)(X-1)}{(X^3-1)(X^2-1)}$, wie man mittels obiger Formel und folgender Tabelle sieht:

d	6	3	2	1
$\mu(\frac{6}{d})$	1	-1	-1	1

Dies kann man auch noch ohne die Formel verifizieren: X^6-1 enthält alle 6-ten Einheitswurzeln, davon zieht man alle zweiten und dritten ab, muss aber die ersten Einheitswurzeln wieder dazu nehmen, denn diese wurden doppelt herausgenommen (bei zweifach und bei dreifach).)

Gekürzt ergibt sich: $f_6(X) = \frac{X^3+1}{X+1} = X^2 - X + 1$.

Für $n = 20$ ergibt sich die Tabelle:

d	20	10	5	4	2	1
$\mu(\frac{20}{d})$	1	-1	0	-1	1	0

und damit $f_{20} = \frac{(X^{20}-1)(X^2-1)}{(X^{10}-1)(X^4-1)} = \frac{X^{10}-1}{X^2+1} = X^8 - X^6 + X^4 - X^2 + 1$.

Bemerkung (Polynome und Einheitswurzeln): Die Polynome $f_n(X)$ aus (10.7) haben Koeffizienten in $\mathbb{Q}$, und sogar in $\{\pm 1, 0\}$, falls $n \leq 104$. Letzteres gilt aber nicht allgemein.

Definition/Proposition 10.8 (formale Dirichlet-Reihen): Eine **formale Dirichlet-Reihe** ist eine Reihe der Form

$$\sum_{n=1}^{\infty} n^{-s} = \sum_{n \geq 1} a_n n^{-s} \quad (a_n \in \mathbb{C}).$$

Ist f eine arithmetische Funktion, so heißt

$$\sum_{n \geq 1} f(n) n^{-s} =: D(f,s)$$

die zugehörige Dirichlet-Reihe. Zu je zwei Dirichlet-Reihen $D(f,s)$ und $D(g,s)$ sind $D(f,s) + D(g,s) = D(f+g,s)$ und $D(f,s) \cdot D(g,s) = D(h,s)$ mit $h(n) = \sum_{\substack{d,m \in \mathbb{N} \\ dm=n}} f(d)g(m) = \sum_{d|\, n} f(d) g(\frac{n}{d})$ wieder formale Potenzreihen. Deshalb bildet die Menge aller formalen Potenzreihen einen kommutativen, nullteilerfreien(!) Ring, d.h. einen Integritätsbereich.

Definition/Proposition 10.9 (Faltung):

Es sei $\mathfrak{A} := \{f | f \text{ ist arithmetische Funktion }\}$ und $\mathfrak{D} = \{f | f \text{ ist formale Dirichlet-Reihe}\}$.

Dann ist $\begin{array}{c} \mathfrak{A} \to \mathfrak{D} \\ f \mapsto D(f,s) \end{array}$ bijektiv. Die dadurch auf $\mathfrak{A}$ definierte Multiplikation "$*$" ist

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

Sie macht $\mathfrak{A}$ zu einen kommutativen nullteilerfreien Ring. Die Verknüpfung "$*$" heißt **Faltung**.

Satz 10.10 (arithmetische Funktionen und Multiplikativität): Sei $f \in \mathfrak{A}$. Dann gilt:

1. f ist Einheit $\Leftrightarrow f(1) \neq 0$
2. f ist multiplikativ $\Leftrightarrow D(f,s)$ besitzt eine formale Produktentwicklung, d.h.

$$D(f,s) = \prod_{p \in \mathbb{P}} \left(1 + \sum_{e \geq 1} f(p^e) p^{-es}\right)$$

3. Die Menge $\mathfrak{M}$ der multiplikativen arithmetischen Funktionen ist eine Untergruppe der multiplikativen Gruppe $\mathfrak{A}^*$ von $\mathfrak{A}$.

Beweis :

1. Das Einselement bzgl. "$*$" ist $\delta : \mathbb{N} \to \mathbb{C},\ n \mapsto \begin{cases} 1 & n=1 \\ 0 & n>1 \end{cases}$

   Die Gleichung $f * g = \delta$ ist äquivalent zu:

   $$\forall\ n \text{ gilt: } \sum_{d|\ n} f\left(\frac{n}{d}\right) g(d) = \begin{cases} 1 & n=1 \\ 0 & n>1 \end{cases}$$

   Ist nun $f(1) \neq 0$, so kann man rekursiv nach g auflösen und erhält:
   $g(1) = f(1)^{-1}, g(n) = -f(1)^{-1} \sum_{\substack{d|\ n \\ d \neq n}} f\left(\frac{n}{d}\right) g(d)$.

   Ist $f(1) = 0$, so ist die Gleichung für kein g erfüllt, denn man erhält die Gleichung $f(1)g(1) = 0$.

2. Es ist klar, daß das Produkt rechts ein wohldefiniertes Element von $\mathfrak{D}$ ist. Ist $n = \prod_{1 \leq i \leq s} p_i^{e_i}$ die Primfaktorzerlegung von n, dann ist der Koeffizient $f(n)$ von n^{-s} in diesem Produkt gerade $\prod_{1 \leq i \leq s} f(p_i^{e_i})$. Dies zeigt, daß die Funktion f mit dieser Produktentwicklung multiplikativ ist.

   Ist umgekehrt f multiplikativ (d.h. $f(n) = \prod_{q \leq i \leq s} f(p_i^{e_i})$, so hat $D(f,s)$ die Produktentwicklung wie in (2.)

3. $\mathfrak{M} \subset \mathfrak{A}^*$ ist klar nach (1.). Daß $\mathfrak{M} \subset \mathfrak{A}$ auch eine Untergruppe ist, bleibt dem Leser als Übung überlassen.

□

Beispiel 10.11 (Faltung):

Sei $\underline{1} \in \mathfrak{A}$ die Funktion von $\mathbb{N} \to \mathbb{C},\ n \mapsto 1$.

(Achtung: Dies ist nicht das Einselement von $\mathfrak{A}$!).

Weiter seien j und j^k die arithmetischen Funktionen mit $j : n \mapsto n$ und $j^k : n \mapsto n^k$. Dann gilt:

- $\underline{1} * \underline{1} = \tau$, denn $(\underline{1} * \underline{1})(n) = \sum_{d|\ n} 1 \cdot 1 = \sigma_0(n) = \tau(n)$.
- $\underline{1} * j = \sigma_1 = \sigma$
- $\underline{1} * j^k = \sigma_k$
- $\underline{1} * \mu = \delta$, denn $(\underline{1} * \mu)(n) = \sum_{d|\ n} 1 \cdot \mu\left(\frac{n}{d}\right) = \sum_{d|\ n} \mu(d) \overset{10.3}{=} \delta(1)$

Mit anderen Worten: Die Faltung mit $\underline{1}$ bewirkt eine Möbius-Transformation, die Faltung mit μ eine inverse Möbius-Transformation.

Definition/Satz 10.12 (von Mangoldt-Funktion): Sei $\lambda : \mathbb{N} \to \mathbb{C}$ die arithmetische Funktion $\lambda := \mu * \log$.
λ heißt die **von Mangoldt-Funktion**. Weiter sei $\psi : \mathbb{R}_{\geq 0} \to \mathbb{C}$ definiert durch $\psi(x) := \sum_{n \leq x} \lambda(n)$ und
$\vartheta : \mathbb{R}_{\geq 0} \to \mathbb{C}, \vartheta(x) = \sum_{p \leq x} \log p$. ψ und ϑ heißen Tschebyschew-Funktionen. Beispielweise ist für $n = 17$:

$$\begin{array}{rcccl} \vartheta(x) = & \log 2 + & \log 3 + & \log 5 + \log 7 + \log 11 + \log 13 + \log 17 \\ \psi(x) = & 4\log 2 + & 2\log 3 + & \log 5 + \log 7 + \log 11 + \log 13 + \log 17 \end{array}$$

Es gelten:

1. $\lambda(n) = \begin{cases} \log p & n = p^e (\leftarrow \text{ Primzahlpotenz}) \\ 0 & \text{sonst} \end{cases}$
2. $\psi(x) = \sum_{p^e \leq x} \log p = \log \text{kgV}\{n \leq x\}$
3. $\psi(x) = \sum_{n \geq 1} \vartheta(\sqrt[n]{x})$ $(\leftarrow$ endliche Summe!)
4. $\vartheta(x) \leq [x] \log 4$
5. $\psi(x) \geq [x] \log 2$
6. $\psi(x) = \vartheta(x) + O(\sqrt{x} \log x)$

Beweis :

1. Es gilt:

$$\lambda(n) = \sum_{d|\,n} \mu(d) \log\left(\frac{n}{d}\right) = \underbrace{\left(\sum_{d|\,n} \mu(d)\right)}_{=\delta(n)=0,\text{wenn } n>1} \log n - \sum_{d|\,n} \mu(d) \log d$$

$$\rightsquigarrow \lambda = -\mu \log * \underline{1}$$

Sind jetzt $m, n > 1$ teilerfremd, so ist

$$\begin{aligned}\lambda(mn) &= -\sum_{d|\,n} \mu(d) \log d \\ &= -\sum_{d_1|\,m} \mu(d_1) \sum_{d_2|\,n} \mu(d_2)(\log d_1 + \log d_2) \\ &= -\sum_{d_1|\,m} \mu(d_1)[\delta(n) \log d_1 - \lambda(n)] \\ &= \delta(n)\lambda(m) + \lambda(n)\delta(m) = 0\end{aligned}$$

Also verschwindet λ auf n, sofern n keine Primzahlpotenz ist. Weiter ist

$$\begin{aligned}\lambda(p^e) &= -(\mu \log * 1)(p^e) \\ &= -(\mu(1)\log 1 + \mu(p)\log p + \sum_{2 \le i \le e} \mu(p^i) \log p^i) \\ &= \log p\end{aligned}$$

2. Ist klar nach (1.).

3. Für $p \in \mathbb{P}$ gilt: $p^e \le x \Leftrightarrow p \le \sqrt[e]{x}$. Deshalb tritt $\log p$ als Summand auf beiden Seiten gleich oft auf.

4. Folgt aus (8.4)

5. Folgt aus (8.5) (wenn man dort Logarithmen zieht)

6. Aus (3.) wissen wir:

$$\psi(x) = \vartheta(x) + \sum_{2 \le n \le \frac{\log x}{\log 2}} \vartheta(\sqrt[n]{x}) = \vartheta(x) + \frac{\log x}{\log 2} O(\sqrt{x}) = \vartheta(x) + O(\sqrt{x}\log x) = \vartheta(x) + O(\sqrt{x}\log x)$$

□

Satz 10.13 (Vermutung von Bertrand): Für alle natürlichen Zahlen n existiert eine Primzahl p mit $n < p \le 2$. Dieser Satz wurde zuerst von Tschebyschew bewiesen.

Beweis : Annahme: $\exists\ n \in \mathbb{N}$ mit: $\nexists\ p \in \mathbb{P}$ mit $n < p \le 2n$. Wir zeigen, daß dann $n \le C$ ist (mit einer geeigneten Konstanten C) und erledigen den Rest "von Hand".

1. Sei $N := \binom{2n}{n}$ und p sei ein Primfaktor von N. Dann gilt:

$$0 < v_p(N) = v_p((2n)!) - 2v_p(n!) \overset{8.1}{=} \sum_{i \ge 1} \left(\left[\frac{2n}{p^i}\right] - 2\left[\frac{n}{p^i}\right] \right)$$

2. Nach Voraussetzung ist $p \le 2n$, also sogar $p \le n$ (wegen unserer Annahme).

3. Es ist sogar $p \leq \frac{2}{3}n$, denn sonst gilt:

$$\begin{aligned}\frac{2}{3}n < p \leq n &\rightsquigarrow 2p \leq 2n < 3p \\ &\rightsquigarrow 9p^2 > 4n^2 \\ &\rightsquigarrow p^2 > \frac{4}{9}n^2 \underset{n>4}{>} 2n \\ &\rightsquigarrow v_p(N) = \left[\frac{2n}{p}\right] - 2\left[\frac{n}{p}\right] = 2 - 2 = 0 \quad \text{Widerspruch.}\end{aligned}$$

4. Also ist jeder Primteiler p von N kleiner als $\frac{2}{3}n$. Deshalb gilt:

$$\sum_{p|\ N} \log p \leq \sum_{p \leq \frac{2}{3}n} \log p = \vartheta\left(\frac{2}{3}n\right) = \vartheta\left(\left[\frac{2}{3}n\right]\right) \overset{10.12}{\leq} \log 4\left[\frac{2}{3}n\right] \leq \frac{4}{3}n\log 2.$$

5. Weiter gilt:

$$v_p(N) \leq \underbrace{\frac{\log(2n)}{\log p}}_{\text{Anzahl der Summanden in der Summe in 1.}},$$

denn für $x \in \mathbb{R}$ gilt: $[2x] - 2[x] \leq 1$. Ist $v_p(N) \geq 2$, so folgt: $2\log p \leq v_p(N)\log p \leq \log 2n$, d.h. $p \leq \sqrt{2n}$, und es gibt höchstens $\sqrt{2n}$ viele solcher p. Also gilt:

$$\sum_{p|\ N, v_p(N)\geq 2} v_p(N)\log p \leq \sqrt{2n}\log 2n.$$

6. Es gilt:

$$\log N = \sum_{p|\ N} v_p(N)\log p = \sum_{\substack{p|\ N \\ v_p(N)=1}} v_p(N)\log p + \sum_{\substack{p|\ N \\ v_p(N)\geq 2}} v_p(N)\log p \overset{(4),(5)}{\leq} \frac{4}{3}n\log 2 + \sqrt{2n}\log 2n.$$

7. $N = \binom{2n}{n}$ ist der größte Term in

$$2^{2n} = (1+1)^{2n} = 1 + \binom{2n}{1} + \binom{2n}{2} + \ldots + \binom{2n}{2n-1} + 1 = \underbrace{2 + \binom{2n}{1} + \binom{2n}{2} + \ldots + \binom{2n}{2n-1}}_{2n \text{ Summanden}}$$

$$\begin{aligned}&\rightsquigarrow 2^{2n} \leq 2n\binom{2n}{n} = 2nN \quad \text{(vgl. 8.3)} \\ &\rightsquigarrow 2n\log 2 \leq \log 2n + \log N \overset{(6.)}{\leq} \log 2n + \frac{4}{3}\log 2 + \sqrt{2n}\log 2n \\ &\rightsquigarrow \frac{2}{3}n\log 2 \leq (1+\sqrt{2n})\log 2n \\ &\rightsquigarrow 2n\log 2 \leq 3(1+\sqrt{2n})\log 2n\end{aligned}$$

Diese Ungleichung hat die Form "$O(n) \leq O(\sqrt{n}\log n)$". Es ist also klar, daß sie ab einem bestimmten n nicht mehr gelten kann.

8. Annahme: $n > 2^9 = 512$. Setze $x := \frac{\log n - 9\log 2}{10\log 2} > 0$. Dann ist $2^{10+10x} = 2^{10}2^{\frac{\log n}{\log 2}}2^{-9} = 2n$. Die letzte Ungleichung aus (7.) wird dann zu:

$$\begin{aligned}2^{10+10x}\log 2 &\leq 3(1+2^{5+5x})(10+10x)\log 2 \\ \rightsquigarrow 2^{10+10x} &\leq 30(1+2^{5+5x})(1+x) \\ \overset{:2^{10}2^{5x}}{\rightsquigarrow} 2^{5x} &\leq \underbrace{30\cdot 2^{-5}}_{<(1-2^{-5})}\underbrace{(1+2^{-5(1+x)})}_{\leq(1+2^{-5})}(1+x) < 1 + x(1-2^{-10}) < 1+x\end{aligned}$$

Andererseits gilt: $2^{5x} = exp(5x\log 2) = 1 + \underbrace{\frac{5\log 2}{1!}}_{>1} x +$ positive Terme. Widerspruch. Also ist $n < 512$.

9. Betrachte die Primzahlen $q_1, q_2, q_3 \ldots = 2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631$. Dann ist jeweils $q_{i+1} < 2q_i$. Also gibt es für jedes $n \leq 630$ ein q_i aus der Liste mit $n < q_i \leq 2n$.

□

11 Mittlere Ordnungen arithmetischer Funktionen

Definition 11.1 (Mittlere Ordnung): Sei $f : \mathbb{N} \to \mathbb{C}$ eine arithmetische Funktion und g eine elementare reelle Funktion. Wir sagen, daß f mittlere Ordnung g hat, falls gilt:

$$(*) \quad \sum_{n\leq x} f(n) \sim \sum_{n\leq x} g(n).$$

Bemerkung (Zu mittleren Ordnungen):

1. "Elementare Funktion" ist nicht wohldefiniert und steht in etwa für "leicht berechenbar".
2. f kann verschiedene mittlere Ordnungen haben.
3. Hat f mittlere Ordnung g, und ist die Approximation in $(*)$ "genügend gut", so beschreibt $g(x)$ den Mittelwert von f in der Umgebung von x, d.h.

$$\frac{\sum_{\substack{n\in\mathbb{N} \\ x-y\leq n\leq x+y}} f(n)}{2y} \approx g(x) \qquad 0 \ll y \ll x$$

4. Bestimmung einer mittleren Ordnung g für f ist äquivalent zur Bestimmung von $\sum_{n\leq x} f(n) = G(x) +$ Fehlerterm mit Abschätzung.

Beispiel (Mittlere Ordnung): Sei $f(n) = \begin{cases} 1 & n \in \mathbb{P} \\ 0 & n \notin \mathbb{P} \end{cases}$, also $\sum_{n\leq x} f(n) = \pi(x)$. $\pi(x) \sim \frac{x}{\log x}$ bedeuted, daß $f(n)$ die mittlere Ordnung $g(x) = \left(\frac{x}{\log x}\right)' \sim \frac{1}{\log x}$ hat.

Proposition 11.2 (Mittlere Ordnung der τ-Funktion): Mit $\tau(n) = \#\{d \in \mathbb{N} : d \mid n\}$ gilt:

$$\sum_{n\leq x} \tau(n) = \sum_{n\leq x}\sum_{d\mid n} 1 = \sum_{d\leq x}\sum_{\substack{n\leq x \\ n\equiv 0(d)}} 1 = \sum_{d\leq x}\left[\frac{x}{d}\right] = \sum_{d\leq x}\left(\frac{x}{d} + O(1)\right) = \underbrace{x\sum_{d\leq x}\frac{1}{d}}_{\log x + O(1)} + \underbrace{[x]O(1)}_{O(x)} = x\log x + O(x).$$

□

Proposition 11.3 (Andere Darstellung von $\sum_{n\leq x} f*g$): Seien f, g zwei arithmetische Funktionen mit summatorischen Funktionen F und G[16]. Für $1 \leq y \leq x$ gilt:

$$\sum_{n\leq x} f*g(n) = \sum_{n\leq y} g(n)F\left(\frac{x}{n}\right) + \sum_{m\leq \frac{x}{y}} f(m)G\left(\frac{x}{m}\right) - F\left(\frac{x}{y}\right)G(y).$$

[16] d.h. $F(x) = \sum_{n\leq x} f(n),\ x \in \mathbb{R}$, analog für g und G.

Beweis : Es gilt:

$$\sum_{n\le x} f*g(n) = \sum_{\substack{m,d\in\mathbb{N}\\ md=n\\ n\le x}} f(m)g(d) = \sum_{\substack{md\le x\\ d\le y}} f(m)g(d) + \sum_{\substack{md\le x\\ d>y}} f(m)g(d)$$
$$= \sum_{d\le y} g(d)F\left(\frac{x}{d}\right) + \sum_{m\le \frac{x}{y}} f(m)\left(G\left(\frac{x}{m}\right) - G(y)\right)$$

□

Eine Verfeinerung von 11.2 ist

Satz 11.4 (Summe über $\tau(n)$): Es gilt:

$$\sum_{n\le x}\tau(n) = x\log x + (2\gamma-1)x + O(\sqrt{x}).$$

Beweis : Wende (11.3) an mit $f,g = \underline{1}$, $F(x) = G(x) = [x]$, $y = \sqrt{x}$. Dann gilt wegen $\tau = \underline{1}*\underline{1}$:

$$\sum_{n\le x}\tau(n) = 2\sum_{m\le\sqrt{x}}\left[\frac{x}{m}\right] - \left[\sqrt{x}\right]^2 = 2x \underbrace{\sum_{m\le\sqrt{x}}\frac{1}{m}}_{\log\sqrt{x}+\gamma+O(x^{-1/2})} + O(\sqrt{x}) - x + O(\sqrt{x})$$
$$= x\log x + 2\gamma x + O(\sqrt{x}) - x + O(\sqrt{x}) = x\log x + (2\gamma-1)x + O(\sqrt{x})$$

□

Folge: Die mittlere Ordnung von $\tau(n)$ ist $\frac{d}{dx}(x\log x + (2\gamma-1)x) = \log x + 2\gamma$.

Beispiel (Mittlere Ordnung von $\tau(n)$): Für $x = 100$ gilt: $\log(100) + 2\gamma = 5,759\ldots$, und das lokale Mittel von $\tau(n)$ für $90 \le n \le 110$ ist $\frac{123}{21} = 5,857\ldots$.

Satz 11.5 (Asymptotik von $\sum_{n\le x}\sigma(n)$): Für $x\to\infty$ gilt:

$$\sum_{n\le x}\sigma(n) = \frac{\pi^2}{12}x^2 + O(x\log x)$$

Beweis : Es gilt:

$$\sum_{n\le x}\sigma(n) = \sum_{n\le x}\sum_{d\mid n} d = \sum_{md\le x} d = \sum_{m\le x}\sum_{d\le\frac{x}{m}} d = \frac{1}{2}\sum_{m\le x}\left[\frac{x}{m}\right]\left(\left[\frac{x}{m}+1\right]\right)$$
$$= \frac{1}{2}\sum_{m\le x}\frac{x^2}{m^2} + O(x\underbrace{\sum_{m\le x}\frac{1}{m}}_{\log x+O(1)}) = \frac{1}{2}x^2\sum_{m\le x}\frac{1}{m^2} + O(x\log x)$$
$$= \frac{1}{2}x^2\left(\sum_{m\in\mathbb{N}}\frac{1}{m^2} - \underbrace{\sum_{m>x}\frac{1}{m^2}}_{O(x^{-1})}\right) + O(x\log x) = \frac{1}{2}\zeta(2)x^2 + O(x) + O(x\log x) = \frac{\pi^2}{12}x^2 + O(x\log x)$$

□

Bemerkung (Mittlere Ordnung von $\sigma(n)$): $\sigma(n)$ hat als mittlere Ordnung $\frac{d}{dx}\left(\frac{\pi^2}{12}x^2\right) = \frac{\pi^2}{6}x$.

Frage: Welche mittlere Ordnung hat $\frac{\sigma(n)}{n}$?

Bemerkung 11.6 (Multiplikativität bei mittleren Ordnungen?): Sind f_1, f_2 arithmetische Funktionen mit mittleren Ordnungen g_1, g_2, so gilt im Allgemeinen nicht: $g_1g_2 =$ mittlere Ordnung von f_1f_2.

Trotzdem gilt:

Satz (Mittlere Ordnung von $\frac{\sigma(n)}{n}$): $\frac{\sigma(n)}{n}$ hat $\frac{\pi^2}{6}$ als mittlere Ordnung.

Beweis : Es gilt:

$$\sum_{n\le x}\frac{\sigma(n)}{n}=\sum_{\substack{m,d\in\mathbb{N}\\ md\le x}}\frac{1}{m}=\sum_{m\le x}\frac{1}{m}\left[\frac{x}{m}\right]=\sum_{m\le x}\frac{1}{m}\left(\frac{x}{m}-\left\{\frac{x}{m}\right\}\right)$$
$$=x\sum_{m\le x}\frac{1}{m^2}+O(\log x)=x\zeta(2)+O(1)+O(\log x)=x\zeta(2)+O(\log x)$$

Damit folgt, daß $\frac{\sigma(n)}{n}$ die mittlere Ordnung $\frac{d}{dx}(x\zeta(2))=\zeta(2)=\frac{\pi^2}{6}$ hat.

Definition 11.7 (Mittelbar): Hat $f\in\mathfrak{A}$ eine konstante mittlere Ordnung $c\in\mathbb{C}$, d.h. $\sum_{n\le x}f(n)\sim cx$, so ist $\lim_{x\to\infty}\frac{1}{x}\sum_{n\le x}f(n)=c$. In diesem Fall heißt f **mittelbar** mit Mittel c. Beispielsweise ist $\frac{\sigma(n)}{n}$ mittelbar mit Mittel $\zeta(2)=\frac{\pi^2}{6}$.

Satz 11.8 (Mittlere Ordnung von $\varphi(n)$): Für $x\to\infty$ gilt:

$$\sum_{n\le x}\varphi(n)=\frac{3}{\pi^2}x^2+O(x\log x)$$

Beweis : Wegen $\sum_{d|\,n}\varphi(d)=n$ ist $\varphi(n)=\sum_{d|\,n}\mu(d)\frac{n}{d}=\sum_{dm=n}\mu(d)m$, und deshalb gilt

$$\sum_{n\le x}\varphi(n)=\sum_{n\le x}\sum_{dm=n}\mu(d)m=\sum_{d\le x}\mu(d)\sum_{m\le\frac{x}{d}}m=\frac{1}{2}\sum_{d\le x}\mu(d)\left[\frac{x}{d}\right]\left(\left[\frac{x}{d}\right]+1\right)$$
$$=\frac{1}{2}x^2\underbrace{\sum_{d\le x}\frac{\mu(d)}{d^2}}_{\substack{\zeta(2)^{-1}+O(x^{-1})\\ \text{s. unten}}}+O(x\log x)=\frac{1}{2}\zeta(2)^{-1}x^2+O(x)+O(x\log x)=\frac{1}{2}\zeta(2)^{-1}x^2+O(x\log x).$$

Wegen $\mu*\underline{1}=\delta$ gilt: $\underbrace{D(\mu,s)}_{=\sum_{n\ge1}\mu(n)n^{-s}}\cdot\underbrace{D(\underline{1},s)}_{=\sum_{n\ge1}n^{-s}}=1$. (= Konstante Dirichlet-Reihe mit Wert 1)

Da beide Summen absolut konvergieren für $s=2$, gilt auch $\left(\sum_{n\ge1}\mu(n)n^{-2}\right)\underbrace{\left(\sum_{n\ge1}n^{-2}\right)}_{=\zeta(2)=\frac{\pi^2}{6}}=1$,

also $\sum_{n\ge1}\mu(n)n^{-2}=\frac{6}{\pi^2}$.

□

$\varphi(n)$ hat folglich die mittlere Ordnung $\frac{6}{\pi^2}x$.

Korollar 11.9 (Mittel von $\frac{\varphi(n)}{n}$): $\frac{\varphi(n)}{n}$ ist mittelbar mit Mittel $\zeta(2)^{-1}=\frac{6}{\pi^2}$.

Beweis : Es gilt:

$$\sum_{n\le x}\frac{\varphi(n)}{n}=\sum_{n\le x}\frac{1}{n}\sum_{d|\,n}\mu(d)\frac{n}{d}=\sum_{d|\,n}\mu(d)\sum_{m\le\frac{x}{d}}\frac{m}{md}=\sum_{d|\,n}\mu(d)\sum_{m\le\left[\frac{x}{d}\right]}\frac{1}{d}=\sum_{d\le x}\mu(d)\left[\frac{x}{d}\right]\frac{1}{d}=\sum_{d\le x}\frac{\mu(d)}{d}\left(\frac{x}{d}-\left\{\frac{x}{d}\right\}\right)$$
$$=x\sum_{d\le x}\frac{\mu(d)}{d^2}+O\left(\sum_{d\le x}\frac{1}{d}\right)=x\left(\zeta(2)^{-1}+O(x^{-1})\right)+O(\log x)$$
$$=\zeta(2)^{-1}x+O(1)+O(\log x)=\zeta(2)^{-1}x+O(\log x)$$

□

Korollar 11.10 (Verifizierung von (7.3)): Die Wahrscheinlichkeit $P(m,n$ teilerfremd) für zwei zufällig gewählte natürliche Zahlen m und n, teilerfremd zu sein, ist $\zeta(2)^{-1} = \frac{6}{\pi^2}$.

Beweis :

$$\begin{aligned} P(m,n \text{ teilerfremd}) &= \lim_{x\to\infty} \frac{\#\{(m,n) \in \mathbb{N}\times\mathbb{N} | m,n \le x (m,n) = 1}{\#\{(m,n) \in \mathbb{N}\times\mathbb{N} | m,n \le x} \\ &= \lim_{x\to\infty} \frac{1 + 2\sum_{n\le x} \varphi(n)}{[x]^2} \quad \text{(Beachte: } \#\{m > n \ldots\} = \#\{m < n \ldots\} = \varphi(n), \#\{m = n \ldots\} = 1) \\ &= \lim_{x\to\infty} \frac{\frac{6}{\pi^2}x^2 + O(x\log x) + 1}{[x]^2} = \frac{6}{\pi^2} \end{aligned}$$

□

Satz 11.11 (Verifizierung von (7.3)): Die Wahrscheinlichkeit $P(n$ quadratfrei), daß eine zufällig gewählte natürliche Zahl n quadratfrei ist, ist ebenfalls $\zeta(2)^{-1}$. (Dies ist keine unmittelbare Folgerung aus 11.10!)

Beweis :

1. n quadratfrei $\Leftrightarrow \mu(n) = \pm 1 \Leftrightarrow \mu(n)^2 = 1$, d.h.

$$P(n \text{ quadratfrei}) = \lim_{x\to\infty} \frac{\#\{n \le x | n \text{ quadratfrei}\}}{\#\{n \le x\}} = \lim_{x\to\infty} \frac{\sum_{n\le x} \mu(n)^2}{[x]} = \text{ Mittel von } \mu(n)^2.$$

2. Für $n \in \mathbb{N}$ ∃! Darstellung $n = qm^2$, $\quad q$ quadratfrei, $q = \prod_{\substack{p|\, n \\ v_p(n) \text{ ungerade}}} p$.

   Dann ist

   - $$\mu(n)^2 = \delta(m) = \sum_{d|\, m} \mu(d),$$
   - und für $d \in \mathbb{N}$ gilt: $d|\, m \Leftrightarrow d^2|\, n$.

3. Deshalb gilt:

$$\begin{aligned} \sum_{n\le x} \mu(n)^2 &= \sum_{n\le x} \sum_{d^2|\, n} \mu(d) = \sum_{d\le\sqrt{x}} \mu(d) \underbrace{\left[\frac{x}{d^2}\right]}_{\left(\frac{x}{d^2} - \left\{\frac{x}{d^2}\right\}\right)} \\ &= x \sum_{d\le\sqrt{x}} \frac{\mu(d)}{d^2} + O(\sqrt{x}) = x\left(\zeta(2)^{-1} + O(x^{-1/2})\right) + O(\sqrt{x}) = x\zeta(2)^{-1} + O(\sqrt{x}) \end{aligned}$$

4. Abschließend gilt:

$$P(n \text{ quadratfrei}) = \lim_{x\to\infty} \frac{\zeta(2)^{-1}x + O(\sqrt{x})}{[x]} = \zeta(2)^{-1}.$$

□

Beispiel (Wahrscheinlichkeit für Quadratfreiheit): Von den ersten 10 Zahlen sind 70% quadratfrei, und unter den ersten 100 Zahlen sind 61% quadratfrei.

Dieser Wert liegt also schon nahe an $\zeta(2)^{-1} \approx 0,607$.

Satz 11.12 (Summe über $\omega(n)$): Es gilt:

$$\sum_{n\le x} \omega(n) = x\log\log x + c_1 x + O\left(\frac{x}{\log x}\right).$$

Beweis : Es ist

$$\sum_{n\le x}\omega(n)=\sum_{n\le x}\sum_{p\mid n}1=\sum_{\substack{p\le x\\ p\in\mathbb{P}}}\left[\frac{x}{p}\right]=\sum_{p\le x}\frac{x}{p}-\sum_{p\le x}\left\{\frac{x}{p}\right\}=x\sum_{p\le x}\frac{1}{p}+O(\pi(x))=x\sum_{p\le x}\frac{1}{p}+O\left(\frac{x}{\log x}\right)$$
$$\overset{9.7}{=}x\left(\log\log x+c_1+O\left(\frac{1}{\log x}\right)\right)+O\left(\frac{1}{\log x}\right)=x\log\log x+c_1x+O\left(\frac{x}{\log x}\right)$$

□

Satz 11.13 (Summe über $\Omega(n)$): Es gilt:

$$\sum_{n\le x}\Omega(n)=x\log\log x+c_2x+O\left(\frac{x}{\log x}\right).$$

Beweis :

1. Wir definieren
$$A(x):=\sum_{n\le x}\Omega(n)-\omega(n)=\sum_{p\in\mathbb{P}}\sum_{k\ge 2}\left[\frac{x}{p^k}\right]$$
und setzen
$$c_2:=c_1+\sum_{p\in\mathbb{P}}\underbrace{\frac{1}{p(p-1)}}_{\text{abs. konvergent}}.$$

2. Es gilt:
$$A(x)\le x\sum_{p\in\mathbb{P}}\sum_{k\ge 2}p^{-k}=x\sum_{p\in\mathbb{P}}\frac{p^{-2}}{1-p^{-1}}=x\sum_{p\in\mathbb{P}}\frac{1}{p(p-1)}=x(c_2-c_1)$$

3. Weiter ist
$$\sum_{2\le k\le\left[\frac{\log x}{\log p}\right]=:n}\frac{1}{p^k}\overset{\text{geom. Summe}}{=}\frac{1-p^{1-n}}{p(p-1)}=\frac{1}{p(p-1)}+O(p^{-n}),$$
und wegen
$$p^{-n}=p^{-\left[\frac{\log x}{\log p}\right]}=e^{-\log p\left[\frac{\log x}{\log p}\right]}$$
gilt
$$O(p^{-n})=O(e^{-\log x})=O(x^{-1}).$$

4. Nun ist
$$\begin{aligned}A(x)&\ge\sum_{p\le\sqrt{x}}\sum_{2\le k\le\frac{\log x}{\log p}}\left(\frac{x}{p^k}-1\right)\overset{3.}{=}x\sum_{p\le\sqrt{x}}\left(\frac{1}{p(p-1)}+O(x^{-1})\right)+x\sum_{p\le\sqrt{x}}O\left(\frac{\log x}{\log p}\right)\\&=x\sum_{p\le\sqrt{x}}\frac{1}{p(p-1)}+O(\sqrt{x})+O(\log x\sqrt{x})=x\sum_{p\le\sqrt{x}}\frac{1}{p(p-1)}+O(\log x\sqrt{x})\\&=x\left(\sum_{p\in\mathbb{P}}\frac{1}{p(p-1)}+O(x^{-1/2})\right)+O(\sqrt{x}\log x)=x(c_2-c_1)+O(\sqrt{x})+O(\sqrt{x}\log x)\\&=x(c_2-c_1)+O(\sqrt{x}\log x)\end{aligned}$$

5. Zusammengefasst ergibt sich:
$$A(x)=(c_2-c_1)x+O(\sqrt{x}\log x)$$
und damit
$$\sum_{n\le x}\Omega(n)=\sum_{n\le x}\omega(n)+A(x)\overset{11.12}{=}x\log\log x+c_1x+O\left(\frac{x}{\log x}\right)+A(x)=x\log\log x+c_2x+O\left(\frac{x}{\log x}\right).$$

□

Es ist $c_1 = \gamma - c_0 = 0,26149\ldots$ und $c_2 = c_1 + \sum_{p\in\mathbb{P}} \frac{1}{p(p-1)} = 1,03465\ldots$.

Der Erwartungwert für $\left\{ \begin{array}{c} \omega(n) \\ \Omega(n) \end{array} \right\}$ für $n \in \mathbb{N}, n \approx x \in \mathbb{R}$ ist also

$$\frac{d}{dx}\left(x\log\log x + \left\{ \begin{array}{c} c_1 \\ c_2 \end{array} \right\}\right) = \log\log x + \frac{1}{\log x} + \left\{ \begin{array}{c} c_1 \\ c_2 \end{array} \right\}.$$

Für $x = 10^{100}$ ergibt sich: $\left\{ \begin{array}{c} 5,7050\ldots \\ 6,4781\ldots \end{array} \right\}$.

Tabelle 11.14 (Summe über $\omega(n)$ und $\Omega(n)$, lokale Mittel etc.):

x	100	1000	10000
$\sum_{n\le x}\omega(n)$	171	2126	24300
$x\log\log x + c_1 x$	$178,\ldots$	$2194,\ldots$	$24818,\ldots$
$\sum_{n\le x}\Omega(n)$	239	2877	31985
$x\log\log x + c_2 x$	$256,\ldots$	$2967,\ldots$	$32549,\ldots$
Lokales MIttel von $\omega(n)$	$1,952\ldots$	$2,262\ldots$	$2,537\ldots$
Erwartungwert für $\omega(n)$	$2,005\ldots$	$2,339\ldots$	$2,590\ldots$

Schlußbemerkung 11.15 (Überblick über mittlere Ordnungen): Der Erwartungwert für die arithmetischen Funktionen $f(n)$ auf einem zufällig gewählten n in der Nähe von $x \gg 0$ ist gegeben durch:

$f(n)$	Erwartungwert = mittlere Ordnung von x	Bewiesen in
$\tau = \sigma_0$	$\log x + 2\gamma$	11.4
$\sigma = \sigma_1$	$\zeta(2)x$	11.5
$\sigma_k, k \ge 2$	$\zeta(k+1)x^k$	nicht bewiesen, Übung
$\frac{\sigma(n)}{n}$	$\zeta(2)$	11.6
φ	$\zeta(2)^{-1}x$	11.8
$\frac{\varphi(n)}{n}$	$\zeta(2)^{-1}$	11.9
$\mu(n)^2$	$\zeta(2)^{-1}$	11.11
χ_r	$\zeta(r)^{-1}$	nicht bewiesen, Übung
ω	$\log\log x + c_1 + \frac{1}{\log x}$	11.12
Ω	$\log\log x + c_2 + \frac{1}{\log x}$	11.13

Dabei ist χ_r die charakteristische Funktion der Menge $\{n \in \mathbb{N} | (m^r \mid n) \Rightarrow (m = 1)\}$, d.h. $\chi_2 = \mu^2$.

12 Extremale Ordnungen

Definition 12.1 (Maximalordnung): Sei f eine reellwertige arithmetische Funktion, $g : \mathbb{R}_{\ge 0} \to \mathbb{R}_{\ge 0}$ monoton wachsend. Dann ist g **Maximalordnung** von f wenn gilt:

$$\overline{\lim_{n\to\infty}} \frac{f(n)}{g(n)} = 1.$$

g ist **Minimalordnung** von f wenn gilt:

$$\underline{\lim_{n\to\infty}} \frac{f(n)}{g(n)} = 1.$$

Satz 12.2 (Grenzwerte über Primzahlpotenzen): Sei $f \in \mathfrak{A}$ multiplikativ. Aus

$$\lim_{\substack{q\to\infty \\ q=p^e, e\in\mathbb{N}, p\in\mathbb{P}}} f(q) = 0$$

folgt $\lim_{n\to\infty} f(n) = 0$.

Beweis : q sei immer eine Primzahlpotenz. Gegeben sei $\varepsilon > 0$.

Es existiert $Q = Q(e)$ mit $q > Q \Rightarrow |f(q)| \leq \varepsilon$. Setze

$$Q_1 := \{q | q \leq Q, |f(q)| \leq 1\}$$
$$Q_2 := \{q | q \leq Q, |f(q)| > 1\}$$
$$Q_3 := \{q > Q\}$$

Jedes $n \in \mathbb{N}$ besitzt eine eindeutige Zerlegung $n = n_1 n_2 n_3$, wobei die n_i paarweise teilerfremd sind und n_i nur exakte Teiler q_i mit $q_i \in Q_i$ enthält.

Es gilt:

- $f(n) = f_1(n_1) f_2(n_2) f_3(n_3)$
- $|f(n_1)| < 1$
- $|f(n_2)| \leq A$ (= Konstante, unabhängig von ε)
- $|f(n_3)| \leq \varepsilon$ (oder $|f(n_3)| = 1$, falls $n_3 = 1$ gilt. Dies kann aber nur für endlich viele n gelten)

$\rightsquigarrow \overline{\lim}_{n\to\infty} |f(n)| \leq \varepsilon A$ gilt für alle ε mit $0 < \varepsilon < 1$.

$\rightsquigarrow \overline{\lim}_{n\to\infty} |f(n)| = 0$

□

Korollar 12.3 (O-Klasse von $\tau(n)$): Für alle $\varepsilon > 0$ gilt $\tau(n) = O_\varepsilon(n^\varepsilon)$. Dabei bedeutet (O_ε), daß die implizierte Konstante von ε abhängt.

Beweis : Setze $f(n) := \tau(n) n^{-\varepsilon}$. Dann ist f multiplikativ und es gilt:

$$f(p^r) = \tau(p^r) p^{-r\varepsilon} = (r+1) p^{-r\varepsilon} \underset{p^r\to\infty}{\to} 0,$$

d.h. $f(q) \underset{q\to\infty}{\to} 0$, also $f(n) \underset{n\to\infty}{\to} 0$ und $\tau(p^r) = O(p^{r\varepsilon})$.

□

Satz 12.4 (Maximalordnung von $\log\tau(n)$): Die Funktion $\log\tau(n)$ hat $\log 2 \frac{\log n}{\log\log n}$ als Maximalordnung. (Die Minimalordnung von $\tau(n)$ ist 2.)

Beweis : Sei n gegeben. Für reelle t mit $2 \leq t \leq n$ gilt:

$$\tau(n) = \prod_{p^i \| n} (i+1) \leq \prod_{\substack{p^i \| n \\ p \leq t}} (\underbrace{i}_{\leq \frac{\log n}{\log 2}} + 1) \prod_{\substack{p^i \| n \\ p > t}} 2^i \leq \left(1 + \frac{\log n}{\log 2}\right)^t \underbrace{\left(\prod_{\substack{p^i \| n \\ p > t}} p^i\right)^{\frac{\log 2}{\log t}}}_{\leq n = exp(\log n)}$$

$$\leq exp\left(t(2 + \log\log n) + \frac{\log 2 \log n}{\log t}\right)$$

Dabei haben wir verwendet:

$$1 \leq \left(e^2 - \frac{1}{\log 2}\right) y \text{ gilt für genügend große } y$$
$$\Rightarrow 1 + \frac{y}{\log 2} \leq e^2 y$$
$$\Rightarrow \log\left(1 + \frac{y}{\log 2}\right) \leq 2 + \log y$$
$$\overset{y=\log n}{\Rightarrow} \log\left(1 + \frac{\log n}{\log 2}\right) \leq 2 + \log\log n$$
$$\Rightarrow \left(1 + \frac{\log n}{\log 2}\right)^t \leq exp(t(2 + \log\log n))$$

Wähle nun $t = \frac{\log n}{(\log\log n)^3}$. Dann gilt:

$$\textbf{12.4.1} \qquad \tau(n) \leq exp\left(\frac{\log 2\log n}{\log\log n}\left(1+O\left(\frac{\log\log\log n}{\log\log n}\right)\right)\right)$$

Der Term $\frac{\log\log\log n}{\log\log n}$ geht gegen Null für n gegen unendlich. Deshalb folgt daraus die erste der folgenden zwei Behauptungen, die wir zeigen müssen:

- $$\forall\, \varepsilon > 0 \exists\, n_0(\varepsilon) \forall\, n \geq n_0 : \tau(n) < exp\left((1+\varepsilon)\log 2\frac{\log n}{\log\log n}\right).$$
- $$\forall\, \varepsilon > 0 : \tau(n) > exp\left((1-\varepsilon)\log 2\frac{\log n}{\log\log n}\right) \text{ für unendlich viele } n.$$

Um die zweite Behauptung zu zeigen finden wir natürliche Zahlen n mit "vielen" Teilern. Wähle dafür $n_k = \prod_{j\leq k} p_j,\ p_1p_2p_3\ldots = 2,3,5\ldots$. Dann gilt: $\tau(n_k) = 2^k$ und

$$\log n_k = \sum_{p\leq p_k} \log p = \vartheta(p_k) \leq k\log p_k \rightsquigarrow \log\tau(n_k) = k\log 2 \geq \log 2\frac{\log n_k}{\log p_k}$$

Erinnerung (10.12): $\vartheta(x) = \psi(x) + O(\sqrt{x}\log x), \psi(x) \geq [x]\log 2$. Daraus folgt: Für alle $a \in \mathbb{R}$ mit $a < \log 2$ ist $\vartheta(x) \geq ax\ \forall\, x \overset{a}{\gg} 0$. Wende dies an für $x = p_k$. Dann folgt für $k \gg 0$:

$$\log(n_k) = \vartheta(p_k) \geq ap_k \rightsquigarrow \log\log n_k \geq \log a + \log p_k$$

$$\rightsquigarrow \log\tau(n_k) \geq \frac{\log 2\log(n_k)}{\log\log n_k\left(1-\frac{\log a}{\log\log n_k}\right)} = \frac{\log 2\log n_k}{\log\log n_k}\left(1+O\left(\frac{1}{\log\log n_k}\right)\right)$$

$$\textbf{14.4.2} \qquad \log\tau(n_k) \geq \frac{\log 2\log n_k}{\log\log n_k}\left(1+O\left(\frac{1}{\log\log n_k}\right)\right)$$

Dies zeigt die zweite Behauptung.

□

Satz 12.5 (Maximalordnung von ω und Ω):

1. Die Maximalordnung von $\omega(n)$ ist $\frac{\log n}{\log\log n}$.
2. Die Maximalordnung von $\Omega(n)$ ist $\frac{\log n}{\log 2}$.
3. Die Minimalordnung von $\omega(n)$ und $\Omega(n)$ ist 1.

Beweis :

1. Für $n = p^i$ ist $\omega(n) = 1, \tau(n) = i+1, \Omega(n) = i$. Deshalb und wegen der Multiplikativität der arithmetischen Funktionen gilt:
$$(*) \qquad 2^{\omega(n)} \underset{(i)}{\leq} \tau(n) \underset{(ii)}{\leq} 2^{\Omega(n)} \underset{(iii)}{\leq} n.$$
Alle Ungleichungen sind optimal: In (i) und (ii) gilt die Gleichheit, wenn $\mu(n)^2 = 1$ und in (iii) gilt die Gleichheit, wenn n eine Zweierpotenz ist.
Aus (12.4.1) und $(*)$ ergibt sich:
$$\omega(n) \leq \frac{\log\tau(n)}{\log 2} \overset{(12.4.1)}{\leq} \frac{\log n}{\log\log n}\left(1+O\left(\frac{\log\log\log n}{\log\log n}\right)\right).$$
Dies zeigt die Abschätzung von (1.). Daß diese Abschätzung scharf ist, folgt aus (14.4.2).
2. Wegen $(*)$ gilt $\Omega(n) \leq \frac{\log n}{\log 2}$, und diese Schranke wird angenommen für $n = 2^k$.
3. klar.

□

Inhaltsverzeichnis

Index