ZAHLENTHEORIE

Skriptum zur Vorlesung
von
Prof. Michael DRMOTA

Inhaltsverzeichnis

Kapitel 1

Teilbarkeit in ganzen Zahlen

1.1 Größter gemeinsamer Teiler und kleinstes gemeinsames Vielfaches

Definition 1.1.1 Seien $a, b \in \mathbb{Z}$. a heißt *teilbar* durch b (a teilt b, b ist Vielfaches von a), wenn es ein $q \in \mathbb{Z}$ mit $a \cdot q = b$ gibt.
Man schreibt dafür auch $a|b$.

Lemma 1.1.1

1. $a|b,\ c \in \mathbb{Z} \ \Rightarrow \ a|b \cdot c$
2. $a|b \ \wedge \ a|c$, $\beta, \gamma \in \mathbb{Z} \ \Rightarrow \ a|\beta \cdot b + \gamma \cdot c$
3. $a|b \ \wedge \ b|a \ \Rightarrow \ a = \pm b$

Satz 1.1.1 Für je zwei ganze Zahlen a, b mit $b \neq 0$ gibt es ganze Zahlen q, r mit $a = q \cdot b + r$, wobei $0 \leq r < |b|$ gilt.
(q heißt Quotient und r Rest.)

Definition 1.1.2 Seien $a, b \in \mathbb{Z}$. Eine ganze Zahl $d > 0$ heißt *größter gemeinsamer Teiler* von a, b, wenn folgende zwei Eigenschaften erfüllt sind:

1. $d|a \ \wedge \ d|b$
2. $t|a \ \wedge \ t|b \ \Rightarrow t|d.$

Man schreibt dafür $d = \mathrm{ggT}(a, b)$ oder $d = (a, b)$.

Definition 1.1.3 Seien $a, b \in \mathbb{Z}$. Eine ganze Zahl $v > 0$ heißt *kleinstes gemeinsames Vielfaches* von a, b, wenn folgende zwei Eigenschaften erfüllt sind:

1. $a|v \ \wedge \ b|v$
2. $a|w \ \wedge \ b|w \ \Rightarrow \ v|w.$

Man schreibt dafür $v = \mathrm{kgV}(a, b)$ oder $v = [a, b]$.

Satz 1.1.2 Zu je zwei ganzen Zahlen a, b gibt es einen eindeutig bestimmten größten gemeinsamen Teiler d. Weiters gibt es ganze Zahlen x, y mit $ax+by = d$.

Definition 1.1.4 Zwei ganze Zahlen a, b heißen *teilerfremd*, wenn $(a, b) = 1$ ist.

Lemma 1.1.2 Ist d der größte gemeinsame Teiler von a, b, so sind $\frac{a}{d}, \frac{b}{d}$ teilerfremd: $(a, b) = d \ \Rightarrow \ (\frac{a}{d}, \frac{b}{d}) = 1$.

Lemma 1.1.3 $(a, b) = 1 \ \wedge \ a|b \cdot c \ \Rightarrow \ a|c.$

Satz 1.1.3 Zu je zwei ganzen Zahlen a, b gibt es ein eindeutig bestimmtes kleinstes gemeinsames Vielfaches v. Weiters gilt $v = \frac{a \cdot b}{(a,b)}$.

Definition 1.1.5 Seien $a_j, \ 1 \le j \le n$, ganze Zahlen. Eine ganze Zahl $d > 0$ heißt größter gemeinsamer Teiler von $a_j, \ 1 \le j \le n$, wenn folgende zwei Eigenschaften erfüllt sind:

1. $d|a_j, \ 1 \le j \le n$
2. $t|a_j, \ 1 \le j \le n \ \Rightarrow \ t|d.$

Man schreibt dafür auch $d = \mathrm{ggT}(a_1, \ldots, a_n)$ oder $d = (a_1, \ldots, a_n)$. Entsprechend heißt eine ganze Zahl $v > 0$ kleinstes gemeinsames Vielfaches von $a_j, \ 1 \le j \le n$, wenn folgende zwei Eigenschaften erfüllt sind:

1. $a_j|v, \ 1 \le j \le n$
2. $a_j|w, \ 1 \le j \le n \ \Rightarrow \ v|w.$

Man schreibt dafür auch $v = \mathrm{kgV}(a_1, \ldots, a_n)$ oder $v = [a_1, \ldots, a_n]$.

Satz 1.1.4 Zu jeder Auswahl von ganzen Zahlen $a_j, \ 1 \le j \le n$, gibt es eindeutig bestimmte größte gemeinsame Teiler $d = (a_1, \ldots, a_n)$ und kleinste gemeinsame Vielfache $v = [a_1, \ldots, a_n]$.
d und v lassen sich rekursiv bestimmen, etwa durch

$$\begin{aligned} d &= (a_1, \ldots, a_n) = ((\ldots((a_1, a_2), a_3)\ldots), a_n) \\ v &= [a_1, \ldots, a_n] = [[\ldots[[a_1, a_2]a_3]\ldots], a_n]. \end{aligned}$$

Weiters gibt es ganze Zahlen $x_j, \ 1 \le j \le n$ mit

$$a_1 x_1 + \ldots + a_n x_n = d.$$

1.2 Fundamentalsatz der Zahlentheorie

Definition 1.2.1 Eine ganze Zahl $p > 1$ heißt *Primzahl*, wenn sie nur die *trivialen Teiler* $\pm 1, \pm p$ hat.
Die Menge aller ganzzahligen Primzahlen wird durch $\mathbb{P}$ bezeichnet.

Lemma 1.2.1 $p \in \mathbb{P} \ \wedge \ p|a \cdot b \ \Rightarrow \ p|a \ \vee \ p|b$

Satz 1.2.1 (Fundamentalsatz der Zahlentheorie) Jede natürliche Zahl n läßt sich bis auf die Reihenfolge eindeutig als Produkt von Primzahlen darstellen.

Bemerkung 1.2.2 Jede natürliche Zahl n läßt sich daher auch durch

$$n = \prod_{p \in \mathbb{P}, p|n} p^{\nu_p(n)}$$

repräsentieren, wobei $\nu_p(n)$ die *Vielfachheit* von $p \in \mathbb{P}$ in n bezeichnet. Definiert man für jene $p \in \mathbb{P}$ mit p teilt nicht $n \quad \nu_p(n) = 0$, so erhält man auch formal das unendliche Produkt

$$n = \prod_{p \in \mathbb{P}} p^{\nu_p(n)}.$$

Satz 1.2.2 $|\mathbb{P}| = \infty$

Satz 1.2.3

$$(a_1, \ldots, a_n) = \prod_{p \in \mathbb{P}} p^{\min(\nu_p(a_1), \ldots, \nu_p(a_n))}$$

$$[a_1, \ldots, a_n] = \prod_{p \in \mathbb{P}} p^{\max(\nu_p(a_1), \ldots, \nu_p(a_n))}$$

Satz 1.2.4 (Wilson) Für $m > 1$ gilt: $m \in \mathbb{P} \ \Leftrightarrow \ m|(m-1)! + 1$.

Bemerkung 1.2.3 Führt man die *Kongruezschreibweise* $a \equiv b \ (m)$ für $m|b-a$ ein, so kann $m|(m-1)!+1$ auch durch $(m-1)! \equiv -1 \ (m)$ dargestellt werden.

1.3 Gaußsche ganze Zahlen

Definition 1.3.1 $\mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\}$ wird als Menge der *Gaußschen ganzen Zahlen* bezeichnet. Bezüglich der gewöhnlichen Addition

$$(a + bi) \ + \ (c + di) \ = \ (a + c) \ + \ (b + d)i$$

und der gewöhnlichen Multiplikation

$$(a + bi) * (c + di) \ = \ (ac - bd) \ + \ (ad + bc)i$$

ist $\mathbb{Z}$ ein *Integritätsbereich.*
$N(a + ib) \ = \ |a + ib|^2 \ = \ (a + ib) * (a - ib) \ = \ a^2 + b^2$ wird als *Norm* von $a + ib$ bezeichnet.
$z_1 \ = \ a + ib \ \in \mathbb{Z}[i]$ heißt *teilbar* durch $z_2 \ = \ c + id \ \in \mathbb{Z}[i]$, wenn es ein $z_3 \ = \ e + if \ \in \mathbb{Z}[i]$ mit $z_1 * z_3 \ = \ z_2$ gibt. Man schreibt auch $z_1 | z_2$.

Lemma 1.3.1

1. $z_1, z_2 \ \in \mathbb{Z}[i], \ z_1 | z_2 \ \Rightarrow \ N(z_1) | N(z_2) \ \ (\in \mathbb{Z})$

2. $N(z) \ = \ 1 \ \Leftrightarrow \ z \in \{\pm 1, \pm i\}$.

3. $z_1 | z_2 \ \wedge \ z_2 | z_1 \ \Rightarrow \ z_1 \ = \ \varepsilon * z_2, \ \varepsilon \in \{\pm 1, \pm i\}$

Satz 1.3.1 Für je zwei *Gaußsche ganze Zahlen* $z_1, z_2 \ \in \mathbb{Z}[i]$ mit $z_2 \neq 0$ gibt es $q, r \in \mathbb{Z}[i]$ mit $z_1 \ = \ q * z_2 + r$, wobei $N(r) < N(z_2)$ gilt.

Bemerkung 1.3.2 *Satz 1.3.1* ist das Analogon zu *Satz 1.1.1*, der grundlegend für alle weiteren Eigenschaften (*Sätze 1.1.2 - 1.2.3*) ist. Es gelten daher die entsprechenden Eigenschaften auch für $\mathbb{Z}[i]$. Insbesondere gibt es eine bis auf die Reihenfolge und mögliche Faktoren $\pm 1, \pm i$ eindeutige Primfaktorzerlegung.

Lemma 1.3.3 Für $p \in \mathbb{P}$ ist die Kongruenz $x^2 \equiv -1 \ (p)$ genau dann lösbar, wenn $p \not\equiv 3 \ (4)$. Für $p = 2$ ist $x = 1$ Lösung und für $p \equiv 1 \ (4) \ \ x = \pm(\frac{p-1}{2})!$
.

Lemma 1.3.4 Für $p \in \mathbb{P}$ und $x \in \mathbb{Z}$ gibt es $a, b \in \mathbb{Z}$ mit $|a| < \sqrt{p}, \ |b| < \sqrt{p}$ und $ax \equiv b \ (p)$.

Lemma 1.3.5 Sind $a, b, c, d \in \mathbb{Z}$ mit $0 < a < b$ und $0 < c < d$, so dass $a^2 + b^2 \ = \ c^2 + d^2 \ \in \mathbb{P}$, dann gilt $a = c$ und $b = d$.

Satz 1.3.2 Für jede Primzahl $p \in \mathbb{P}$ mit $p \equiv 1\ (4)$ gibt es eindeutig bestimmte natürliche Zahlen $a < b$ mit $a^2 + b^2 = p$.

Satz 1.3.3 Die Primzahlen in $\mathbb{Z}[i]$ sind

1. $\pm 1, \pm i$,
2. $\varepsilon * p$ mit $\varepsilon \in \{\pm 1, \pm i\}$, und $p \in \mathbb{P},\ p \equiv 3\ (4)$, und
3. $\varepsilon * (a + ib)$ mit $\varepsilon \in \{\pm 1, \pm i\}$ und $a^2 + b^2 = p\ \in \mathbb{P}, p \equiv 1\ (4)$.

Satz 1.3.4 Eine natürliche Zahl n ist genau dann als Summe zweier Quadrate ganzer Zahlen darstellbar, wenn alle Primteiler $p \in \mathbb{P}$ von n mit $p \equiv 3\ (4)$ in gerader Vielfachheit $\nu_p(n) \equiv 0\ (2)$ auftreten.

Kapitel 2

Kongruenzen

2.1 Die Eulersche φ-Funktion

Definition 2.1.1 Seien $a, b \in \mathbb{Z},\ m \in \mathbb{N}$. Man sagt *a ist kongruent zu „b modulo m "*, $a \equiv b\ (m)$, wenn $m|(a-b)$.
Die Menge

$$\bar{a} = \{b \in \mathbb{Z}|\ a \equiv b\ (m)\} = a + m\mathbb{Z}$$

heißt die von a erzeugte *Restklasse modulo m*.
Auf den Restklassen wird duch

$$\overline{a} + \overline{b} = \overline{a+b},\ \overline{a} * \overline{b} = \overline{a * b}$$

eine Addition und eine Multiplikation erklärt.
Bezeichnet man mit $\mathbb{Z}_m$ die Menge aller Restklassen *modulo m*, so ist $|\mathbb{Z}_m| = m$ und $\langle \mathbb{Z}_m, +, * \rangle$ ein kommutativer Ring mit Einselement.
Die *Einheitengruppe* $\mathbb{Z}_m^*$ besteht aus jenen Restklassen $\bar{a}$, die ein multiplikatives Inverses besitzen. Ihre Ordnung

$$\varphi(m) \ = \ |\mathbb{Z}_m^*|$$

wird als *Eulersche φ-Funktion* bezeichnet.

Lemma 2.1.1 $a \equiv b\ (m), c \equiv d\ (m) \ \Rightarrow\ a + c \equiv b + d\ (m), a * c \equiv b * d\ (m)$

Lemma 2.1.2 $\bar{a} \ \in\ \mathbb{Z}_m^* \ \Leftrightarrow\ (a, m) = 1$

Folgerung 2.1.1 $\varphi(m) \ = \ |\{1 \leq a \leq m \mid (a, m) = 1\}|$

Satz 2.1.1 $\varphi(m) \ = \ m * \prod_{p \in \mathbb{P},\ p|m} (1 - \frac{1}{p}) \ = \ \prod_{p \in \mathbb{P},\ p|m} p^{\nu_p(m)-1}(p-1)$

Satz 2.1.2 $(m,n) = 1 \Rightarrow \varphi(m*n) = \varphi(m)*\varphi(n)$

Satz 2.1.3 $\sum_{1\leq d\leq m,\ d|m} \varphi(d) = m$

Satz 2.1.4 $\mathbb{Z}_m$ ist Körper $\Leftrightarrow$ $\mathbb{Z}_m$ ist Integritätsbereich $\Leftrightarrow$ $m \in \mathbb{P}$

Satz 2.1.5 (Kleiner Fermatscher Satz) $(a,m) = 1 \Rightarrow a^{\varphi(m)} \equiv 1\ (m)$

Folgerung 2.1.2 $p \notin \mathbb{P},\ p$ teilt nicht $a \Rightarrow a^{p-1} \equiv 1\ (p)$

Folgerung 2.1.3 $p \in \mathbb{P},\ a \in \mathbb{Z} \Rightarrow a^p \equiv a\ (p)$

2.2 Chinesischer Restsatz

Satz 2.2.1 Seien $a,b \in \mathbb{Z},\ m \in \mathbb{N}$. Die Kongruenz $ax \equiv b\ (m)$ ist genau dann lösbar, wenn $(a,m)|b$. In diesem Fall ist die Lösung *modulo* $\frac{m}{(a,m)}$ eindeutig.

Lemma 2.2.1 Seien $m_1, m_2, \ldots, m_r$ paarweise teilerfremd und $a \equiv 0\ (m_j),\ 1 \leq j \leq r$. Dann gilt $a \equiv 0\ (m_1 * m_2 \cdots m_r)$.

Satz 2.2.2 (Chinesischer Restsatz) Seien $m_1, m_2, \ldots, m_r \in \mathbb{N}$ paarweise teilerfremd und $a_1, a_2, \ldots, a_r \in \mathbb{Z}$. Dann gibt es eine Lösung des Kongruenzensystems $x \equiv a_j\ (m_j),\ 1 \leq j \leq r$, die *modulo* $m = m_1 * m_2 \cdots m_r$ eindeutig ist.

Folgerung 2.2.1 Sind $m_1, \cdots, m_r \in \mathbb{N}$ paarweise teilerfrend und bezeichne $m = m_1 * m_2 \cdots m_r$, so gilt

$$\langle \mathbb{Z}_m, +, * \rangle \cong \langle \mathbb{Z}_{m_1}, +, * \rangle \oplus \cdots \oplus \langle \mathbb{Z}_{m_r}, +, * \rangle\ ,$$

also auch

$$\langle \mathbb{Z}_m^*, * \rangle \cong \langle \mathbb{Z}_{m_1}^*, * \rangle \otimes \cdots \otimes \langle \mathbb{Z}_{m_r}^*, * \rangle\ .$$

Bemerkung 2.2.2 Für paarweise teilerfremde $m_1, \cdots, m_r \in \mathbb{N}$ gilt daher

$$\varphi(m) = \varphi(m_1) * \varphi(m_2) \cdots \varphi(m_r)\ ,$$

wie auch aus *Satz 2.1.2* folgt. Weiters reicht es, um $\mathbb{Z}_m^*$ zu charakterisieren, $\mathbb{Z}_{p^e}^*$ für Primzahlen $p \in \mathbb{P}$ zu bestimmen.

2.3 Primitivwurzeln

Definition 2.3.1 Eine natürliche Zahl $g > 1$ heißt Primitivwurzel *modulo* m, wenn die Potenzen von g alle primen Restklassen *modulo* m durchlaufen, d.h. $\bar{g}$ ist erzeugendes Element von $\mathbb{Z}_m^*$.

Satz 2.3.1 (Gauß) Genau für die Module $m = 1, 2, 4, p^e, 2p^e$, wobei p eine ungerade Primzahl ist und $e \geq 1$ ist, gibt es eine Primitivwurzel *modulo* m, d.h. $\mathbb{Z}_m^*$ ist zyklisch.

Lemma 2.3.1 $\mathbb{Z}_p^*$ ist für jede Primzahl p zyklisch.

Lemma 2.3.2 Sei g Primitivwurzel modulo einer Primzahl p. Dann gilt entweder $g^{p-1} \not\equiv 1\ (p^2)$ oder $(g+p)^{p-1} \not\equiv 1\ (p^2)$.

Lemma 2.3.3 Sei g Primitivwurzel modulo einer ungeraden Primzahl p, für die $g^{p-1} \not\equiv 1\ (p^2)$ gilt. Dann ist $g^{p^{k-2}(p-1)} \not\equiv 1\ (p^k)$ für alle $k \geq 2$.

Folgerung 2.3.1 $\mathbb{Z}_{p^e}^*$ und $\mathbb{Z}_{2p^e}^*$ sind für alle ungeraden Primzahlen p und alle $e \geq 1$ zyklisch.

Lemma 2.3.4 Sind $m, n > 2$ zwei teilerfremde natürliche Zahlen mit $(m, n) = 1$, dann ist $\mathbb{Z}_{m \cdot n}^*$ nicht zyklisch.

Satz 2.3.2 $\mathbb{Z}_{2^e}^* = \{\bar{5}, \bar{5}^2, \ldots, \bar{5}^{2^{e-2}}, -\bar{5}, -\bar{5}^2, \ldots, -\bar{5}^{2^{e-2}}\}$ für alle $e \geq 3$.

2.4 Polynomiale Kongruenzen

Satz 2.4.1 Seien $m_1, m_2, \ldots, m_r \in \mathbb{N}$ teilerfremd, $m_1 \cdot m_2, \cdots, m_r$ und $f(x)$ ein ganzzahliges Polynom. Dann ist die Kongruenz $f(x) \equiv 0\ (m)$ genau dann lösbar, wenn die Kongruenzen $f(x) \equiv 0\ (m_1)$, $f(x) \equiv 0\ (m_2), \cdots, f(x) \equiv 0\ (m_r)$ jeweils lösbar sind.

Lemma 2.4.1 Für eine Primzahl p und ein ganzzahliges Polynom $f(x)$ vom Grad n hat die Kongruenz $f(x) \equiv 0\ (p)$ höchstens n inkongruente Lösungen *modulo* p.

Satz 2.4.2 Sei $e > 1$ und seien $n_1, n_2, \ldots, n_k$ ein vollständiges System von *modulo* p^{e-1} inkongruenten Lösungen von $f(x) \equiv 0\ (p^{e-1})$, so erhält man ein vollständiges System von inkongruenten Lösungen von $f(x) \equiv 0\ (p^e)$, indem man für jedes u_j die Zahlen $u_j + vp^{e-1}$ bildet, wobei v alle (*mod* p inkongruenten) Lösungen der linearen Kongruenzen $f'(u_j)v \equiv -\frac{f(u_j)}{p^{e-1}}\ (p)$ durchläuft.

Folgerung 2.4.1 Ist $f(u) \equiv 0\ (p)$ für eine Primzahl p und $f'(u) \not\equiv 0\ (p)$, so sind alle Kongruenzen $f(x) \equiv 0\ (p^e)$ für $e \geq 1$ lösbar.

2.5 Appendix: Die Carmichaelfunktion $\lambda(u)$

Definition 2.5.1 $\lambda(n) = \max\{ord_{\mathbb{Z}_n^*}(a) \mid a \in \mathbb{Z}_n^*\}$

Satz 2.5.1 $\lambda(2) = 1;\ \lambda(4) = 2;\ \lambda(4^e) = 2^{e-2}\ (e \geq 2);$
$\lambda(p^e) = p^{e-1} * (p-1) \qquad (p \in \mathbb{P},\ p \equiv 1\ (2),\ e \geq 1);$
$n = {p_1}^{e_1} \cdots {p_r}^{e_r} \Rightarrow \lambda(n) = \mathrm{kgV}(\lambda({p_1}^{e_1}), \ldots, \lambda({p_r}^{e_r})).$

Kapitel 3

Quadratische Reste

3.1 Legendresymbol

Lemma 3.1.1

1. Eine allgemeine quadratische Kongruenz $ax^2+bx+c = 0\ (m)$ ist genau dann lösbar, wenn die Kongruenz $(2ax+b)^2 \equiv b^2-4ac\ (4am)$ lösbar ist.

2. Sei $m = {p_1}^{e_1} \cdots {p_r}^{e_r}$ die Primfaktorenzerlegung von m. Eine reinquadratische Kongruenz $x^2 \equiv a\ (m)$ ist genau dann lösbar, wenn $x^2 \equiv a\ ({p_j}^{e_j})$ für alle $j = 1, 2, \ldots, r$ lösbar ist.

3. Sei $p \in \mathbb{P}$ und $e \geq 1$. Weiters sei $a = p^f * b$ mit $(b,p) = 1$. Eine reinquadratische Kongruenz $x^2 = a\ (p^e)$ ist für $f < e$ genau dann lösbar, wenn f gerade ist und die Kongruenz $y^2 \equiv b\ (b^{e-f})$ lösbar ist.

4. Sei $p \in \mathbb{P}$ ungerade und $(a,p) = 1$. Ist die Kongruenz $x^2 \equiv a\ (p)$ lösbar, so auch die Kongruenzen $x^2 \equiv a\ (p^e)$ für alle $e \geq 1$.

5. Sei a ungerade. Dann ist die Kongruenz $x^2 \equiv a\ (2)$ immer lösbar, die Kongruenz $x^2 \equiv a\ (4)$ nur im Fall $a \equiv 1\ (4)$ lösbar und schließlich die Kongruenz $x^2 \equiv a\ (2^e)$ für $e \geq 3$ nur im Fall $a \equiv 1\ (8)$ lösbar.

Bemerkung 3.1.2 Die Lösbarkeit allgemeiner quadratischer Kongruenzen ist daher auf den Fall $x^2 \equiv a\ (p)$ (mit $(a,p) = 1$, siehe **(4.)**) zurückgeführt worden. ($p \in \mathbb{P}$ ungerade)

Definition 3.1.1 Sei $p \in \mathbb{P}$ und $(a,p) = 1$. a heißt *quadratischer Rest modulo* p, wenn die Kongruenz $x^2 \equiv a\ (p)$ lösbar ist und *quadratischer*

Nichtrest modulo p, wenn die Kongruenz $x^2 \equiv a\ (p)$ keine Lösung hat. Das *Legendresymbol* $(\frac{a}{p})$ ist durch

$$\left(\frac{a}{p}\right) = \begin{cases} +1, & \text{falls } a \text{ quadratischer Rest modulo } p \text{ ist,} \\ 0, & \text{falls } \mathrm{ggT}(a,p) \neq 1, \text{d.h. } p|a, \\ -1, & \text{falls } a \text{ quadratischer Nichtrest modulo } p \text{ ist.} \end{cases}$$

definiert.

Lemma 3.1.3 Sei g Primitivwurzel *modulo* p ($p \in \mathbb{P}$) ungerade. Dann gilt für alle $k \in \mathbb{N}$

$$\left(\frac{g^{2k}}{p}\right) = 1 \text{ und } \left(\frac{g^{2k+1}}{p}\right) = -1.$$

Lemma 3.1.4

$$\left(\frac{a * b}{p}\right) = \left(\frac{a}{p}\right) * \left(\frac{b}{p}\right)$$

Satz 3.1.1 (Eulersches Kriterium)

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}\ (p). \quad (p \in \mathbb{P} \textit{ ungerade})$$

3.2 Quadratisches Reziprozitätsgesetz

Satz 3.2.1 (1. Ergänzungssatz)

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \quad (p \in \mathbb{P} \text{ ungerade})$$

Lemma 3.2.1 (Gauß) Sei $p \in \mathbb{P}$ ungerade und $(a,p) = 1$. Bezeichnet n die Anzahl der Zahlen der Menge $\{a, 2a, 3a, \dots, \frac{p-1}{2}a\}$, deren Reste bei Division durch p größer als $\frac{p}{2}$ sind, so gilt $\left(\frac{a}{p}\right) = (-1)^n$.

Satz 3.2.2 (2. Ergänzungssatz)

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} \quad (p \in \mathbb{P} \text{ ungerade})$$

Lemma 3.2.2 $p \in \mathbb{P}$ ungerade, a ungerade,

$$(a,p) = 1 \;\Rightarrow\; \left(\frac{a}{p}\right) = (-1)^{\sum_{j=1}^{\frac{p-1}{2}} [\frac{ja}{p}]}.$$

Satz 3.2.3 (Quadratisches Reziprozitätsgesetz) Für verschiedene ungerade Primzahlen $p, q \in \mathbb{P}$ gilt

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

3.3 Jacobisymbol

Definition 3.3.1 Für ganze Zahlen a und ungerade positive Zahlen b mit $(a,b) = 1$ wird das *Jacobisymbol* $\left(\frac{a}{b}\right)$ durch

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right) \cdots \left(\frac{a}{p_l}\right)$$

definiert, wobei $b = p_1 \cdots p_l$ eine Zerlegung von b in nicht notwendigerweise verschiedene Primzahlen ist und $\left(\frac{a}{p_j}\right)$ das *Legendresymbol* bezeichne.

Satz 3.3.1 Für ganze Zahlen a_1, a_2 bzw. ungerade Zahlen b_1, b_2 bzw. a, b gilt

1. $\left(\frac{a_1 a_2}{b}\right) = \left(\frac{a_1}{b}\right) * \left(\frac{a_2}{b}\right)$
2. $\left(\frac{a}{b_1 b_2}\right) = \left(\frac{a}{b_1}\right) * \left(\frac{a}{b_2}\right)$
3. $\left(\frac{-1}{b}\right) = (-1)^{\frac{b-1}{2}}$
4. $\left(\frac{2}{b}\right) = (-1)^{\frac{b^2-1}{2}}$
5. $\left(\frac{a}{b}\right) * \left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2} * \frac{b-1}{2}}$.

Bemerkung 3.3.1 Mit Hilfe des *Jacobisymbols* kann das *Legendresymbol* $\left(\frac{a}{p}\right)$ auch ohne Primfaktorenzerlegung von a berechnet werden.

3.4 Gaußsche Summen *modulo p*

Definition 3.4.1 Sei p eine ungerade Primzahl und $n \not\equiv 0$ (p). Dann wird durch

$$G_p(n) = \sum_{r=1}^{p-1} \left(\frac{r}{p}\right) e^{\frac{2\pi i n r}{p}}$$

die *quadratische Gaußsche Summe modulo p* definiert.

Lemma 3.4.1

1. $G_p(n) = \left(\frac{n}{p}\right) G_p(1)$
2. $G_p(1)^2 = p * \left(\frac{-1}{p}\right)$

Lemma 3.4.2

$$p, q \in \mathbb{P} \text{ ungerade } \Rightarrow \; G_p(1)^{q-1} \; = \; \left(\frac{q}{p}\right) \sum_{r_1=1}^{p-1} \cdots \sum_{r_q=1}^{p-1} \left(\frac{r_1 \cdots r_q}{p}\right), \;\; r_1 + \cdots + r_q \; \equiv \; q \; (p)$$

Lemma 3.4.3

$$p, q \; \in \; \mathbb{P} \text{ ungerade } \; \Rightarrow \; \sum_{r_1=1}^{p} \cdots \sum_{r_q=1}^{p} \left(\frac{r_1 \cdots r_q}{p}\right) \; \equiv \; 1 \; (q), \;\; r_1 + \cdots + r_q \; \equiv \; q \; (p)$$

Satz 3.4.1 $p, q \neq \mathbb{P}$ ungerade $\Rightarrow \; \left(\frac{p}{q}\right) \left(\frac{q}{p}\right) \; = \; (-1)^{\frac{p-1}{2} * \frac{q-1}{2}}$

Satz 3.4.2 (Gauß)

$$G_p(1) = \begin{cases} \sqrt{p} & \text{für } p \; \equiv \; 1 \; (4) \\ i\sqrt{p} & \text{für } p \; \equiv \; 3 \; (4) \; . \end{cases}$$

Kapitel 4

Diophantische Gleichungen

4.1 Lineare diophantische Gleichungen

Satz 4.1.1 Seien $a_1, \ldots, a_n, b \in \mathbb{Z}\backslash\{0\}$. Die *diophantische Gleichung*

$$a_1 x_1 + \cdots + a_n x_n = b \tag{4.1}$$

ist genau dann lösbar, wenn $(a_1, \ldots, a_n) \mid b$.
Sei $\underline{x}^{(0)} = (x_1^{(0)}, \ldots, x_n^{(0)}) \in \mathbb{Z}^n$ eine Lösung. Dann gibt es $n-1$ linear unabhängige ganzzahlige Lösungen $\underline{x}^{(1)}, \ldots, \underline{x}^{(n-1)} \in \mathbb{Z}^n$ der homogenen Gleichung $a_1 x_1 + \cdots + a_n x_n = 0$, so dass alle Lösungen von 4.1 durch

$$\underline{x} = \underline{x}^{(0)} + k_1 \underline{x}^{(1)} + \cdots + k_{n-1} \underline{x}^{(n-1)}$$

mit $k_1, k_2, \ldots, k_{n-1} \in \mathbb{Z}$ gegeben sind.

4.2 Quadratische diophantische Gleichungen

Satz 4.2.1 Sei $P(x, y) \in \mathbb{Q}[x, y]$ ein Polynom zweiten Grades. Dann hat die Gleichung $P(x, y) = 0$ entweder keine rationalen Lösungen oder unendlich viele rationale Lösungen $(x, y) \in \mathbb{Q}^2$.
Im letzteren Fall lassen sich alle Lösungen rational parametrisieren, d.h. es gibt rationale Funktionen $x = \varphi(t),\ y = \psi(t) \quad (t \in \mathbb{Q})$, die alle Lösungen von $P(x, y) = 0$ in $\mathbb{Q}^2$ beschreiben.

Lemma 4.2.1 Sei $Q(x, y, z) \in \mathbb{Z}[a, y, z]$ ein homogenes Polynom zweiten Grades. Dann entsprechen die ganzzahligen Lösungen (x, y, z) der diophantischen Gleichung $Q(x, y, z) = 0$ mit $z \neq 0$ und $(x, y, z) = 1$ genau den rationalen Lösungen der Gleichung $P(x, y) = Q(x, y, 1) = 0$.

Folgerung 4.2.1 Die einzigen Lösungen von $x^2 + y^2 = z^2$ mit $(x, y) = 1$ und $x \equiv 0\ (2)$ sind durch

$$x = 2ab,\ y = a^2 - b^2,\ z = a^2 + b^2$$

mit $a, b \in \mathbb{Z},\ (a, b) = 1$ gegeben.

Satz 4.2.2 Die Gleichung $x^4 + y^4 = z^2$ hat keine ganzzahligen Lösungen mit $x \neq 0$ und $y \neq 0$.

Folgerung 4.2.2 Die *diophantische Gleichung* $x^4 + y^4 = z^4$ hat keine ganzzahligen Lösungen mit $x \neq 0$ und $y \neq 0$.

Satz 4.2.3 Sei D eine positive ganze Zahl, die keine Quadratzahl ist. Dann hat die *Pellsche Gleichung*

$$y^2 - Dx^2 = 1$$

unendlich viele ganzzahlige Lösungen. Sei $x = U,\ y = T$ jene Lösung mit $U > 0,\ T > 0$, wo $x = U$ den kleinstmöglichen Wert hat. Dann lassen sich alle Lösungen $(x, y) \in \mathbb{Z}^2$ durch

$$y + x\sqrt{D} = \pm(T + U\sqrt{D})^n$$

mit $n \in \mathbb{Z}$ darstellen.

Lemma 4.2.2 Sei $\alpha \in \mathbb{R}\backslash\mathbb{Q}$ und $p > 1$ eine ganze Zahl. Dann gibt es $x, y \in \mathbb{Z}$, $0 < x \leq q$ mit

$$|y - \alpha x| < \frac{1}{q}.$$

Lemma 4.2.3 Es gibt unendlich viele Paare $x, y \in \mathbb{Z}$ mit

$$|y^2 - Dx^2| < 1 + 2\sqrt{D}$$

Bemerkung 4.2.4 Hat die *diophantische Gleichung* $y^2 - Dx^2 = k$ ($k \in \mathbb{Z}\backslash\{b\}$) eine Lösung, so hat sie unendlich viele, die sich ähnlich wie in *Satz 4.2.3* aus endlich vielen Basislösungen generieren lassen. Es ist aber bisher ungelöst für welche D und k es überhaupt Lösungen gibt.

4.3 Summen von Potenzen

Satz 4.3.1 = *Satz 1.3.4* Eine natürliche Zahl n ist genau dann als Summe zweier Quadrate ganzer Zahlen darstellbar, wenn alle Primteiler $p \in \mathbb{P}$ von n mit $p \equiv 3$ (4) in gerader Vielfachheit $\nu_p(n) \equiv 0$ (2) auftreten.

Satz 4.3.2 Eine natürliche Zahl n ist genau dann als Summe dreier Quadrate ganzer Zahlen darstellbar, wenn n von der Form $n = 4^k(8j + 7)$ mit $k \geq 0$ und $j \geq 0$ ist.

Satz 4.3.3 (Satz von Lagrange) Jede natürliche Zahl n ist als Summe von vier Quadraten ganzer Zahlen darstellbar.

Lemma 4.3.1 $({a_1}^2 + {a_2}^2 + {a_3}^2 + {a_4}^2)({b_1}^2 + {b_2}^2 + {b_3}^2 + {b_4}^2) = (a_1b_1 + a_2b_2 + a_3b_3 + a_4b_4)^2 + (a_1b_2 - a_2b_1 + a_3b_4 - a_4b_3)^2 + (a_1b_3 - a_3b_1 + a_4b_2 - a_2b_4)^2 + (a_1b_4 - a_4b_1 + a_2b_3 - a_3b_2)^2$

Lemma 4.3.2 Sei $p \in \mathbb{P}$ ungerade. Dann gibt es $x_0,\ y_0 \in \mathbb{Z}$ mit $0 \leq x_0, y_0 \leq \frac{p-1}{2}$, sodass ${x_0}^2 + {y_0}^2 + 1^2 + 0^2 \equiv 0$ (p) ist.

Definition 4.3.1 Sei $k \geq 2$. $g(k)$ ist das Minimum aller $g \in \mathbb{N}$, so dass jede natürliche Zahl als Summe von höchstens g k-ten Potenzen natürlicher Zahlen darstellbar ist. [z.B. $g(2) = 4$]

Lemma 4.3.3 $g(k) \geq 2^k + \left[\left(\frac{3}{2}\right)^k\right] - 2$

Satz 4.3.4 $g(k) \geq 2^k + \left[\left(\frac{3}{2}\right)^k\right] - 2$ für alle $k \geq 2$ mit höchstens endlich vielen Ausnahmen, die, wenn sie überhaupt existieren, alle größer als 471 600 000 sind.

Bemerkung 4.3.4 Die Behauptung $g(k) < \infty$ $(k \geq 2)$ wurde von *Waring* aufgestellt [*Waringsches Problem*], allerdings ist kein Beweis überliefert.
Erst *Hilbert* löste das *Waringsche Problem* $g(k) < \infty$ schlüssig.
Übrigens wurde der Beweis von $g(4) = 19$ erst vor wenigen Jahren erfolgreich erbracht. Der Nachweis, dass es nur höchstens endlich viele Ausnahmen für die Formel von $g(k)$ gibt, stammt von *Mashler*.

Kapitel 5

Kettenbrüche

Definition 5.0.2 Ein rationaler Ausdruck der Form

$$r(a_0, a_1, \ldots, a_n) = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots \, \cfrac{\ddots}{a_{n-1} + \frac{1}{a_n}}}}}$$

heißt *endlicher Kettenbruch* $[a_0, a_1, \ldots, a_n]$. Die a_i heißen *Teilnenner*.

Satz 5.0.5 Definiert man rekursiv Polynome $p_i = p_i(a_0, \ldots, a_i)$, $q_i = q_i(a_0, \ldots, a_i)$ durch

$$p_{-2} = 0, \; p_{-1} = 1, \;\; p_i = a_i p_{i-1} + p_{i-2} \; (i \geq 0)$$

$$q_{-2} = 1, \; q_{-1} = 0, \;\; q_i = a_i q_{i-1} + q_{i-2} \; (i \geq 0),$$

so gilt

$$[a_0, a_1, \ldots, a_n] = \frac{p_n}{q_n}.$$

Satz 5.0.6

$$p_n q_{n-1} - p_{n-1} q_n = (-1)^{n-1}$$

$$p_n q_{n-2} - p_{n-2} q_n = (-1)^n a_n$$

Satz 5.0.7 Ist $a_0 \in \mathbb{Z}$ und $a_n \in \mathbb{N}$ $(n \geq 1)$, so sind p_n, q_n teilerfremde ganze Zahlen (d.h. $(p_n, q_n) = 1$) und $0 < q_0 < q_1 < \ldots$ sind unbeschränkt. Weiters konvergiert die Folge $X_n = [a_0, a_1, \ldots, a_n]$ gegen eine reelle Zahl α. Dieser Grenzwert ist der *unendliche Kettenbruch* $[a_0, a_1, \ldots]$.

Satz 5.0.8 Jede relle Zahl α besitzt eine Kettendruchentwicklung. Sie bestimmt man rekursiv durch $\alpha_0 = \alpha$, $a_n = [\alpha_n]$, $\alpha_{n+1} = \frac{1}{\alpha_n - a_n} = \frac{1}{\alpha_n - [\alpha_n]}$.
Bei irrationalem α entsteht ein unendlicher Kettenbruch, der dieser Zahl eineindeutig entspricht. Bei rationalem α bricht die Kettenbruchentwicklung ab: $\alpha = [a_0, a_1, \ldots, a_n]$ mit $a_n \geq 2$.
Unter der Voraussetzung $a_n \geq 2$ ist die Darstellung eindeutig.
(Im allgemeinen ist $[a_0, a_1, \ldots, a_n - 1, 1]$ auch eine Kettenbruchentwicklung von α. Sonst gibt es keine weiteren.)

Definition 5.0.3 $\alpha \in \mathbb{R}$. Die a_n der Kettenbruchentwicklung heißen *Teilnenner von α* und die Brüche $\frac{p_n}{q_n}$ *Näherungsbrüche von α.*

Satz 5.0.9 $\frac{q_n}{q_{n-1}} = [a_n, a_{n-1}, \ldots, a_1]$. D.h. zwei aufeinanderfolgende Nenner von Näherungsbrüchen bestimmen den Anfangsabschnitt der Kettenbruchentwicklung.

Satz 5.0.10 $\alpha \in \mathbb{R}$, $\alpha_0 = \alpha$, $\alpha_{n+1} = \frac{1}{\alpha_n - [\alpha_n]}$.

1. $a_n \leq \alpha_n < a_n + 1$, für $\alpha \notin \mathbb{Q}:\ a_n < \alpha_n < a_n + 1$.
2. $\alpha_n = [a_n, a_{n+1}, \ldots]$
3. $q_n\alpha - p_n = \frac{(-1)^n}{\alpha_{n+1}q_n + q_{n-1}}$; $q_n\alpha - p_n = \frac{(-1)^n \alpha_{n+2}}{\alpha_{n+2}q_{n+1} + q_n}$
4. $$\left.\begin{array}{r} \frac{1}{2q_{n+1}} \\ \frac{1}{q_n(a_{n+1}+2)} \end{array}\right\} < \frac{1}{q_n + q_{n+1}} < |q_n\alpha - p_n| < \frac{1}{q_{n+1}} < \frac{1}{q_n a_{n+1}} < \frac{a}{q_n}$$

Satz 5.0.11 Gibt es ein $\epsilon > 0$, sodass für unendlich viele $n:\ a_{n+1} > {q_n}^{\epsilon}$ ist, so ist $\alpha = [a_0, a_1, \ldots]$ transzendent.

Satz 5.0.12 (Satz von Hurwitz) Sei $\alpha \notin \mathbb{Q}$. Dann gibt es unendlich viele Brüche $\frac{p}{q}$ mit $|\alpha - \frac{p}{q}| < \frac{1}{\sqrt{5}q^2}$.

Definition 5.0.4 $\frac{a}{b}$ mit $b > 0$ heißt beste Approximation von $\alpha \in \mathbb{R}$, wenn für jeden von $\frac{a}{b}$ verschiedenen Bruch $\frac{c}{d}$ mit $0 < d \leq b$

$$|d\alpha - c| > |b\alpha - a|$$

gilt.

Satz 5.0.13 Jeder Näherungsbruch von α (mit der möglichen Ausnahme $\frac{p_0}{q_0}$) ist eine beste Approximation und umgekehrt.

Satz 5.0.14 Gilt für einen Bruch $\frac{a}{b}$ mit $b > 0$ $|\alpha - \frac{a}{b}| < \frac{1}{b^2}$, so ist $\frac{a}{b}$ Näherungsbruch.

Definition 5.0.5 Ein unendlicher Kettenbruch $[a_0, a_1, \ldots]$ ist *periodisch*, wenn es $j, n \in \mathbb{N}$ mit $a_k = a_{k+n}$ für alle $k \geq j$ gibt.

Satz 5.0.15 Ein unendlicher Kettenbruch ist periodisch genau dann, wenn sein Wert eine quadratische Irrationalzahl ist.

Definition 5.0.6 $\alpha \in \mathbb{R}$ heißt *schlecht approximierbar*, falls es ein $c > 0$ gibt, sodass für alle Brüche $\frac{p}{q}$ $\quad |q\alpha - p| > \frac{c}{q}$ gilt.

Satz 5.0.16 $\alpha \in \mathbb{R}$ ist schlecht approximierbar genau dann, wenn die Teilnenner a_n beschränkt sind.

Satz 5.0.17

$$e = [2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, \ldots], \ a_0 = 2, \ a_{3m} = a_{3m-2} = 1, \ a_{3m+1} = 2m$$

Kapitel 6

Primzahlen

6.1 Zahlentheoretische Funktionen

Definition 6.1.1 Eine Abbildung $a : \mathbb{N} = \{1, 2, 3, \ldots\} \to \mathbb{C}$ heißt *zahlentheoretische Funktion*. Jeder zahlentheoretischen Funktion entspricht eine (formale) *Dirichletsche Reihe*

$$A(s) = \sum_{n=1}^{\infty} \frac{a(n)}{n^s}.$$

Definition 6.1.2 Durch $c(n) = (a + b)(n) = a(n) + b(n)$ wird die *Summe* zweier zahlentheoretischer Funktionen definiert. Ihr entspricht die Dirichletsche Reihe

$$C(s) = \sum_{n=1}^{\infty} \frac{c(n)}{n^s} = \sum_{n=1}^{\infty} \frac{a(n) + b(n)}{n^s} = \sum_{n=1}^{\infty} \frac{a(n)}{n^s} + \sum_{n=1}^{\infty} \frac{b(n)}{n^s} = A(s) + B(s).$$

Definition 6.1.3 Durch

$$c(n) = (a * b)(n) = \sum_{d|n} a(d)b(\frac{n}{d}) = \sum_{d_1 \cdot d_2 = n} a(d_1) \cdot b(d_2)$$

wird das *Dirichletprodukt* zweier zahlentheoretischer Funktionen definiert. Ihm entspricht die Dirichletsche Reihe

$$C(s) = \sum_{n=1}^{\infty} \frac{c(n)}{n^s} = \sum_{n=1}^{\infty} \sum_{d_1 \cdot d_2 = n} \frac{a(d_1)b(d_2)}{{d_1}^s \cdot {d_2}^s} = A(s) \cdot B(s).$$

Satz 6.1.1 Die zahlentheoretischen Funktionen bilden mit $+, *$ einen Integritätsbereich, insbesondere ist $*$ assoziativ und kommutativ. Weiters besteht die Einheitengruppe genau aus jenen zahlentheoretischen Funktionen a mit $a(1) \neq 0$.

Definition 6.1.4 Eine zahlentheoretische Funktion a heißt *multiplikativ*, falls für alle $m, n \geq 1$ mit $(m,n) = 1$ $a(m \cdot n) = a(m) \cdot a(n)$ gilt und $a(0) = 1$ ist.
Eine zahlentheoretische Funktion a heißt *vollständig (oder stark) multiplikativ*, falls für alle $m, n \geq 1$ $a(m \cdot n) = a(m) \cdot a(n)$ gilt und $a(0) = 1$ ist.

Satz 6.1.2 Sind die zahlentheoretischen Funktionen a, b multiplikativ, so auch $a * b$ und a^{-1}.

Bemerkung 6.1.1 Sind a, b vollständig multiplikativ, so ist i.a. $a * b$ bzw. a^{-1} nicht mehr vollständig multiplikativ, aber multiplikativ.

Bemerkung 6.1.2 Multiplikative Funktionen a sind durch die Werte $a(p^k)$, $p \in \mathbb{P}$, $k \geq 1$, wohlbestimmt. Ist $n = {p_1}^{k_1} \cdots {p_l}^{k_l}$, so gilt $a(n) = a({p_1}^{k_1}) \cdots a({p_l}^{k_l})$ und für die Dirichletsche Reihe gilt (formal)

$$A(s) = \sum_{n=1}^{\infty} \frac{a(n)}{n^s} = \prod_{p \in \mathbb{P}} \left(1 + \frac{a(p)}{p^s} + \frac{a(p^2)}{p^{2s}} + \cdots \right).$$

Für vollständig multiplikative Funktionen a gilt überdies, dass sie bereits durch die Werte $a(p)$, $p \in \mathbb{P}$, wohldefiniert sind:

$$a({p_1}^{k_1} \cdots {p_l}^{k_l}) = a(p_1)^{k_1} \cdots a(p_l)^{k_l}.$$

Für die Dirichletsche Reihe gilt daher

$$A(s) = \sum_{n=1}^{\infty} \frac{a(n)}{n^s} = \prod_{p \in \mathbb{P}} \left(1 + \frac{a(p)}{p^s} + \left(\frac{a(p)}{p^s} \right)^2 + \cdots \right) = \prod_{p \in \mathbb{P}} \frac{1}{1 - \frac{a(p)}{p^s}}.$$

Die Produktdarstellung heißt *Eulersches Produkt*.

Spezielle zahlentheoretische Funktionen:
($\mathbb{M}$ ... multiplikative Funktion, $\mathbb{VM}$ ... vollständig multiplikative Funktion)

1.

$$I(n) = S_{n1} = \begin{cases} 1 & n = 1 \\ 0 & n > 1 \end{cases} \in \mathbb{VM} \qquad \sum_{n=1}^{\infty} \frac{I(n)}{n^s} = 1$$

2.

$$J(n) = 1 \text{ für } n \geq 1 \quad \in \mathbb{VM} \qquad \sum_{n=1}^{\infty} \frac{J(n)}{n^s} = \sum_{n=1}^{\infty} \frac{1}{n^s} = \zeta(s)$$

... **Riemannsche Zetafunktion**

3. $N_\alpha(n) = n^\alpha$

$$J = N_0 \quad \in \mathbb{VM} \qquad \sum_{n=1}^{\infty} \frac{N_\alpha(n)}{n^s} = \sum_{n=1}^{\infty} \frac{n^\alpha}{n^s} = \zeta(s-\alpha)$$

4. $d(n) = \sum_{d|n} 1$ ... Anzahl der Teiler von n

$$d = J * J \quad \in \mathbb{M} \qquad \sum_{n=1}^{\infty} \frac{d(n)}{n^s} = \zeta(s)^2$$

5. $\sigma(n) = \sum_{d|n} d$ ... Summe aller Teiler von n

$$\sigma = N_1 * J \quad \in \mathbb{M} \qquad \sum_{n=1}^{\infty} \frac{\sigma(n)}{n^s} = \zeta(s)\zeta(s-1)$$

6. $\sigma_\alpha(n) = \sum_{d|n} d^\alpha$

$$\sigma_\alpha = N_\alpha * J \quad \in \mathbb{M} \qquad \sum_{n=1}^{\infty} \frac{\sigma_\alpha(n)}{n^s} = \zeta(s)\zeta(s-\alpha)$$

7.

$$\mu(n) = \begin{cases} 1 & n = 1 \\ (-1)^k & n = p_1 \cdots p_k \text{ und alle } p_1, \ldots, p_k \text{ verschieden} \\ 0 & sonst \end{cases} \quad \in \mathbb{M}$$

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \frac{1}{\zeta(s)}$$

$\mu * J = I,\ \mu = J^{-1} \in \mathbb{M}$ ... **Möbiussche My-Funktion**

8.

$\phi(n) = |\{k | 1 \leq k \leq n,\ (k,n) = 1\}| \in \mathbb{M}$ ... **Eulersche Phi-Funktion**

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

$$\phi * J = N_1,\ \phi = \mu * N_1,\ \phi(n) = n \prod_{p|n} \left(a - \frac{1}{p}\right),\ \phi^{-1}(n) = n \prod_{p|n} (1-p)$$

9.

$$\lambda(n) = \begin{cases} 1 & n = 1 \\ (-1)^{k_1+\cdots+k_l} & n = {p_1}^{k_1} \cdots {p_l}^{k_l} \end{cases} \in \mathbb{M}$$

...**Liouvillesche Lambda-Funktion**

$$\sum_{n=1}^{\infty} \frac{\lambda(n)}{n^s} = \frac{\zeta(2s)}{\zeta(s)}$$

$$(\lambda * J)(n) = \begin{cases} 1 & n = m^2 \\ 0 & \text{sonst} \end{cases} , \lambda^{-1} = |\mu|$$

10.

$$\Lambda(n) = \begin{cases} \log p & n = p^k \\ 0 & \text{sonst} \end{cases} \notin \mathbb{M} \ \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s} = -\frac{\zeta'(s)}{\zeta(s)}$$

...**Mangoldtsche Lambda-Funktion**
$(\Lambda * J)(n) = \log n$

Satz 6.1.3 Ist a vollständig multiplikativ, so gilt $a^{-1}(n) = a(n) \cdot \mu(n)$.

6.2 Analytischer Beweis des Primzahlsatzes

Definition 6.2.1 $\pi(x) = \sum_{p \le x} 1 = |\{p \in \mathbb{P} | p \le x\}|$
$\vartheta(x) = \sum_{p \le x} \log p$ ...**Tschebyscheffsche ϑ-Funktion**
$\psi(x) = \sum_{p^\nu \le x} \log p$ ...**Tschebyscheffsche ψ-Funktion**

Lemma 6.2.1

$$\frac{\vartheta(x)}{x} \le \frac{\psi(x)}{x} \le \pi(x) \cdot \frac{\log x}{x} \le \frac{1}{\log x} + \frac{\vartheta(x)}{x} \cdot \frac{1}{1 - \frac{2 \log\log x}{\log x}} \le \frac{1}{\log x} + \frac{\psi(x)}{x} \cdot \frac{1}{1 - \frac{2 \log\log x}{\log x}}$$

Satz 6.2.1 $\pi(x) \sim \frac{x}{\log x}\ (x \to \infty) \ \Leftrightarrow\ \vartheta(x) \sim x\ (x \to \infty) \ \Leftrightarrow\ \psi(x) \sim x\ (x \to \infty)$

Satz 6.2.2 $\psi(x) = \mathcal{O}(x)$ $(x \to \infty)$

Folgerung 6.2.1 $\pi(x) = \mathcal{O}(\frac{x}{\log x})$ $(x \to \infty)$

Satz 6.2.3 Die Reihendarstellung $\sum_{n=1}^{\infty} \frac{1}{n^s}$ für die *Riemannsche Zeta-Funktion* $\zeta(s)$ konvergiert für alle $s \in \mathbb{C}$ mit $Re(s) > 1$ absolut und stellt dort eine analytische Funktion dar.
Im selben Bereich $(Re(s) > 1)$ konvergiert das *Eulerprodukt* $\prod_{p \in \mathbb{P}} \frac{1}{1-\frac{1}{p^s}}$ und stimmt dort mit $\zeta(x) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ überein.
Weiters besitzt die Funktion $f(s) = \zeta(s) - \frac{1}{s-1}$ für $Re(s) > 0$ eine analytische Fortsetzung bis auf einen *Pol* 1.*Ordnung* mit *Residuum* 1 an der Stelle $s_0 = 1$. (*meromorphe Fortsetzung*)

Satz 6.2.4 $Re(s) = 1,\ s \neq 1 \Rightarrow \zeta(s) \neq 0.$

Satz 6.2.5 Für $Re(s) > 1$ gilt: $\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s} = s \int_1^{\infty} \psi(x) x^{s-1} dx = -\frac{\zeta'(s)}{\zeta(s)}$.

Bemerkung 6.2.2 Aus *Satz 6.2.3* und *Satz 6.2.4* folgt, dass die Funktion $-\frac{\zeta'(s)}{\zeta(s)}$ (bis auf einen Pol 1. Ordnung mit Residuum 1 an der Stelle $s_0 = 1$) in ein Gebiet fortgesetzt werden kann, das die Gerade $Re(s) = 1$ umfasst.

Satz 6.2.6 Sei $F : (0, \infty) \to \mathbb{C}$ eine beschränkte Funktion, die in jedem kompakten Intervall $I \subseteq (0, \infty)$ integrierbar ist und sei

$$G(z) = \int_0^{\infty} F(t) e^{-zt} dt$$

(*Laplacetransformierte von* $F(t)$) für $t \in \mathbb{C}$ mit $Re(z) > 0$ gegeben. Läßt sich $G(z)$ in ein die Halbebene $\{z \in \mathbb{C} | Re(z) \geq 0\}$ umfassendes Gebiet analytisch fortsetzen, dann existiert das uneigentliche Integral

$$\int_0^{\infty} F(t) dt.$$

Satz 6.2.7 Sei $f : [1, \infty) \to \mathbb{R}$ monoton wachsend und $f(x) = \mathcal{O}(x)$ $(x \to \infty)$. Weiters sei

$$g(s) = s \int_1^{\infty} f(x) x^{-s-1} dx$$

für $s \in \mathbb{C}$ mit $Re(s) > 1$ definiert. Gibt es ein $c > 0$, so dass $g(s) - \frac{c}{s-1}$ in ein die Halbebene $\{s \in \mathbb{C} | Re(s) \geq 1\}$ umfassendes Gebiet analytisch fortgesetzt werden kann, dann gilt:
$f(x) \sim c \cdot x$ $(x \to \infty)$.

Satz 6.2.8 $\psi(x) \sim x$ $(x \to \infty)$

Folgerung 6.2.2 (Primzahlsatz) $\pi(x) \sim \frac{x}{\log x}$ $(x \to \infty)$.