1 Teilbarkeit und Primzahlen

Definition 1.1. Seien $a, b \in \mathbb{Z}, b \neq 0$. a ist durch b *teilbar* $:\Leftrightarrow \exists c \in \mathbb{Z} : a = bc$. b heißt dann ein *Teiler* von a und a ein *Vielfaches* von b. Notation $b|a$.

Definition 1.2. Sei $p \in \mathbb{N}, p \geqslant 2$. p heißt *Primzahl* $:\Leftrightarrow \forall d \in \mathbb{N}$: $d|p \Rightarrow d \in \{1, p\}$. Sonst heißt p *zusammengesetzt*.

Beispiele: 2,3,5, ..., aber nicht 1.

Proposition 1.3. Sei $a \in \mathbb{N}, a \neq 1$. Dann ist a ein Produkt von Primzahlen, d.h. $\exists p_1, \ldots, p_n$ prim (nicht notwendig verschieden): $a = p_1 \cdot \ldots \cdot p_n$.

Theorem 1.4 (Euklid)**.** Es gibt unendlich viele verschiedene Primzahlen.

Definition 1.5. Sei $\mathcal{P} = \{p \in \mathbb{N} : p \text{ prim}\}$. Für $x \in \mathbb{R}$ sei $\pi(x) := \#\{p : p \in \mathcal{P}, p \leqslant x\}$, die *Anzahlfunktion* der Primzahlen, oder die *Primzahlfunktion*.

Theorem 1.6 (Fundamentalsatz der Arithmetik)**.** Sei $n \in \mathbb{N}$. Dann existieren eindeutig bestimmte Zahlen $e(p) \in \mathbb{N}_0$, für jedes $p \in \mathcal{P}$, so dass gilt: $n = \prod_{p \in \mathcal{P}} p^{e(p)}$. Insbesondere sind fast alle $e(p)$ Null. Das heißt, jede natürliche Zahl ist eindeutig darstellbar als Produkt von Primzahlpotenzen.

Proposition 1.7. Für $x \geqslant 2$ gilt $\sum_{p \leqslant x,\ p \in \mathcal{P}} \frac{1}{p} > \ln \ln x - \frac{1}{2}$.

Korollar 1.8. $\prod_{p \in \mathcal{P}} (1 - \frac{1}{p^s})^{-1} = \sum_{n \in \mathbb{N}} \frac{1}{n^s}$ für $s > 1, s \in \mathbb{R}$.

Euler-Produkt $\prod_{p \in \mathcal{P}} (\sum_{k=0}^{\infty} \frac{1}{p^{ks}}) = \sum_{n \in \mathbb{N}} \frac{1}{n^s}$

Definition 1.9. *Die Riemannsche ζ - Funktion* ist definiert durch
$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s}$ für $s \in \mathbb{C}$ mit $\operatorname{Re} s > 1$.

Proposition 1.10. Seien $a, b \in \mathbb{N}, a = p_1^{a_1} \cdot \ldots \cdot p_l^{a_l}, b = p_1^{b_1} \cdot \ldots \cdot p_l^{b_l}$. Dann $\exists! d \in \mathbb{N} : d|a, d|b$ und $\forall e \in \mathbb{N} : e|a$ und $e|b \Rightarrow e|d$. d heißt *größter gemeinsamer Teiler* von a und b. Bezeichnung: $d = ggT(a, b)$.
Außerdem $\exists! k \in \mathbb{N} : a|k,\ b|k$ und $\forall j \in \mathbb{N} : a|j$ und $b|j \Rightarrow k|j$. k heißt *kleinstes gemeinsames Vielfaches* von a und b. Bezeichnung: $k = kgV(a, b)$.
Es gilt: $a \cdot b = ggT(a, b) \cdot kgV(a, b)$.

2 Kongruenzen

Theorem 2.1 (Kleiner Satz von Fermat, 1640)**.** Sei p eine Primzahl, $a \in \mathbb{Z}$. Dann gilt $a^p \equiv a (\text{mod } p)$. Falls $p \nmid a$, gilt $a^{p-1} \equiv 1 (\text{mod } p)$.

Definition 2.2. Die *Eulersche φ - Funktion* ist definiert durch $\varphi : \mathbb{Z} \to \mathbb{N}$, $\varphi(n) := \#\{\overline{a} \in \mathbb{Z}/n\mathbb{Z} : ggT(a, n) = 1\}$.

Theorem 2.3 (Satz von Euler, 1760)**.** Sei $n \in \mathbb{Z}$ und $a \in \mathbb{Z}$ mit $ggT(a,n) = 1$. Dann gilt $a^{\varphi(n)} \equiv 1 (\text{mod } n)$.

Proposition 2.4. Die Eulersche φ-Funktion erfüllt:

(a) $\varphi(n) = n - 1$, wenn $n = p$ prim.

(b) $\varphi(p^a) = p^a - p^{a-1}$ für p prim, $a \geqslant 1$.

(c) $\varphi(ab) = \varphi(a) \cdot \varphi(b)$, falls $(a,b) = 1$.

(d) $\varphi(p_1^{a_1} \cdot p_2^{a_2} \dots p_r^{a_r}) = (p_1^{a_1} - p_1^{a_1-1})(p_2^{a_2} - p_2^{a_2-1}) \dots (p_r^{a_r} - p_r^{a_r-1})$ für $p_1, p_2, \dots, p_r$ paarweise verschiedene Primzahlen.

(e) $\sum_{d|m} \varphi(d) = m$ für jedes m.

Theorem 2.5 (Chinesischer Restsatz, Sun Tsu, zwischen 200 und 470)**.** Seien $m_1, \dots, m_k$ paarweise teilerfremd. Dann gilt für beliebige $a_1, \dots, a_k \in \mathbb{Z}$:

$$x \equiv a_1 (\text{mod } m_1), \dots, x \equiv a_k (\text{mod } m_k)$$

hat genau eine simultane Lösung modulo $m_1 \cdot \dots \cdot m_k$.

Theorem 2.6 (Satz von Wilson)**.** Sei p prim. Dann gilt: $(p-1)! \equiv -1 (\text{mod } p)$.

3 Polynomiale Kongruenzen, Primitivwurzeln und quadratische Reste

Proposition 3.1. Sei p eine Primzahl. Die quadratische Kongruenz $X^2 \equiv -1 \ (mod\ p)$ ist lösbar $\Leftrightarrow p \not\equiv 3 \ (mod\ 4)$.
Für $p = 2$ ist 1 die eindeutige Lösung *modulo* 2.
Für $p \equiv 1 \ mod\ 4$ gibt es *modulo* p genau zwei verschiedene Lösungen, $(\frac{p-1}{2})!$ und $-(\frac{p-1}{2})!$.

Proposition 3.2. $\varphi_f(m) := \{x \in \ \mathbb{Z}/m\mathbb{Z} : f(x) \equiv 0 \ (\text{mod } m)\}$
$\varphi_f(m) = \prod_{k=1}^{e} \varphi_f(p_k^{a_k})$.

Proposition 3.3. Sei $f(x) \in \mathbb{Z}[x]$, p prim, $a \in \mathbb{N}_{\geqslant 2}$ und $y \in \mathbb{Z}$ mit $f(y) \equiv 0 \ (mod\ p^{a-1})$. Dann gilt:

(a) Falls $p | f'(y)$ und $f(y) \neq 0 \ (mod\ p^a)$, dann gibt es kein z mit $f(z) \equiv 0 \ (mod\ p^a)$ und $z \equiv y \ (mod\ p^{a-1})$.

(b) Falls $p | f'(y)$ und $f(y) \equiv 0 \ (mod\ p^a)$, dann gibt es genau p viele z mit $f(z) \equiv 0 \ (mod\ p^a)$ und $z \equiv y \ (mod\ p^{a-1})$.

(c) Falls $p \nmid f'(y)$, dann existiert genau ein z mit $f(z) \equiv 0 \ (mod\ p^a)$ und $z \equiv y \ (mod\ p^{a-1})$.
z hat die Form $z = y + dp^{a-1}$, wobei d die eindeutige Lösung von $f'(y)d \equiv -\frac{f(y)}{p^{a-1}} \ (mod\ p)$ ist.

Theorem 3.4 (Chevalley)**.** Sei $f(x_1, \ldots, x_n) \in \mathbb{Z}\,[x_1, \ldots, x_n]$ mit $deg(f) < n, f(0) = 0$. Dann hat die Kongruenz $f(x_1, \ldots, x_n) \equiv 0\ (mod\ p)$ neben dem Nullvektor noch mindestens eine weitere Lösung.

Definition 3.5. Ein c mit $(c, p) = 1$, so daß ein x existiert mit $x^k \equiv c\ (mod\ p)$ heißt *k-ter Potenzrest modulo p*. Wenn es kein solches x gibt, heißt c *k-ter Potenz-Nichtrest modulo p*. Für $k = 2$ redet man von *quadratischen Resten* und *quadratischen Nichtresten*.

Definition 3.6. Sei p prim und $x \in \mathbb{N}$. x heißt *Primitivwurzel modulo* $p :\Leftrightarrow ord(x) = p - 1$.

Theorem 3.7. Zu jeder Primzahl p existiert eine Primitivwurzel.

Definition 3.8. Sei g eine Primitivwurzel modulo p und $x = g^a$. a heißt der *Index* von x (bzgl. der Primitivwurzel g). Notation: $\mathrm{ind}_p x$

Theorem 3.9. Sei p prim. Die k-ten Potenzreste modulo p sind genau die $a \in \{1, \ldots, p-1\}$, für die gilt: $ggT(k, p-1) | ind\ a$. Es gibt genau $\frac{p-1}{ggT(k,p-1)}$ viele k-te Potenzreste.

4 Quadratische Reziprozität

Definition 4.1 (Legendre)**.** Das *Legendre-Symbol* ist definiert als

$$(\tfrac{a}{p}) := \begin{cases} 1, & \text{wenn } a \text{ quadratischer Rest } mod\ p \\ -1, & \text{wenn } a \text{ quadratischer Nichtrest } mod\ p \end{cases}$$

$\forall a, b \in \mathbb{N} : (\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$.

Theorem 4.2 (Eulers Kriterium)**.** Für alle a mit $a \not\equiv 0\ (mod\ p)$ gilt:
$\left(\frac{a}{p}\right) \equiv a^q\ (mod\ p)$ für $q = \frac{p-1}{2}$.

Korollar 4.3. -1 ist ein quadratischer Rest für Primzahlen $p = 4k + 1$, und ein quadratischer Nichtrest für Primzahlen $p' = 4k + 3$. Für $p = 4k + 1$ gilt also für alle $a : (\frac{a}{p}) = (\frac{p-a}{p})$, während für $p' = 4k + 3$ gilt: $(\frac{a}{p}) = -(\frac{p-a}{a})$.

Lemma 4.4 (Gauß)**.** $(\frac{a}{p}) = (-1)^{\nu}$.

Theorem 4.5. Sei $p = 4ak + r$, mit $0 < r < 4a$ und $p' = 4ak' + r'$, mit $0 < r' < 4\ a$. Dann ist $(\frac{a}{p}) = (\frac{a}{p'})$, falls $r = r'$ oder $r' = 4a - r$.

Theorem 4.6 (Quadratisches Reziprozitätsgesetz, Gauß 1796)**.** Seien p und q verschiedene ungerade Primzahlen. Dann gilt $(\frac{p}{q}) \cdot (\frac{q}{p}) = (-1)^{(p-1)(q-1)/4}$. Das bedeutet:

$$p \equiv q \equiv 1\ (mod\ 4) \Rightarrow (\tfrac{p}{q}) = (\tfrac{q}{p})$$

$$p \equiv q \equiv 3\ (mod\ 4) \Rightarrow (\tfrac{p}{q}) = -(\tfrac{q}{p})$$

$$p \not\equiv q\ (mod\ 4) \Rightarrow (\tfrac{p}{g}) \equiv (\tfrac{q}{p})$$

Falls $p \equiv q \equiv 3\ (mod\ 4)$, ist genau eine der beiden Gleichungen $x^2 \equiv q\ (mod\ p)$ und $x^2 \equiv p (mod\ q)$ lösbar.
Sonst sind immer beide Gleichungen lösbar oder beide nicht lösbar.

5 Summen von Quadraten

Theorem 5.1. Sei $n \in \mathbb{N}$. Dann sind äquivalent:

(1) Die Gleichung $x^2 + y^2 = n$ hat Lösungen $x, y \in \mathbb{N}_0$.

(2) Jeder Primteiler $p|n$ mit $p \equiv 3 \ (mod\ 4)$ kommt in n mit geradem Exponenten vor.

Theorem 5.2. Jede natürliche Zahl $n \in \mathbb{N}$ ist eine Summe von vier Quadraten. D.h. die Gleichung $x^2 + y^2 + z^2 + w^2 = n$ hat Lösungen $x, y, z, w \in \mathbb{N}_0$.

6 Arithmetische Funktionen

Theorem 6.1. Die Wahrscheinlichkeit, dass zwei positive ganze Zahlen teilerfremd sind, beträgt $6/\pi^2$.

Definition 6.2. Eine Funktion $f : \mathbb{N} \to \mathbb{C}$ heißt *arithmetische (oder zahlentheoretische) Funktion*. Seien f und g arithmetische Funktionen.
Dann ist die *punktweise Summe* definiert als $f + g : n \mapsto f(n) + g(n)$.
Das *punktweise Produkt* ist definiert als $f \cdot g : n \mapsto f(n)g(n)$.
Die(Dirichlet-)Faltung ist definiert als $f * g : n \mapsto (f * g)(n) := \sum_{d|n} f(d)\ g(\frac{n}{d}) = \sum_{d_1 d_2 = n} f(d_1)\ g(d_2)$.

Proposition 6.3. Die Menge $\mathcal{A}$ der arithmetischen Funktionen mit punktweiser Addition und Multiplikation durch Dirichlet-Faltung ist ein kommutativer Ring. Die Nullfunktion ist das neutrale Element der Addition. Die δ-Funktion ist das neutrale Element der Multiplikation.

Proposition 6.4. Sei $L(n) := log\ n, L : \mathbb{N} \to \mathbb{C}$. Dann ist punktweise Multiplikation mit L eine Derivation von $\mathcal{A}$, d.h. eine Abbildung $D : \mathcal{A} \to \mathcal{A}$, für die gilt:
$D(xy) = D(x)y + xD(y)\ \forall\ x, y \in \mathcal{A}$.

Definition 6.5. Die *Möbius-Funktion* ist definiert durch

$$\mu(n) = \begin{cases} 1 & n = 1 \\ (-1)^k & n = p_1 \cdots p_k,\ p_i \neq p_j \text{ für } i \neq j, \text{ alle prim } (n \text{ quadratfrei}) \\ 0 & \exists p \text{ prim} : p^2 | n \end{cases}$$

Proposition 6.6. Die Möbius-Funktion ist multiplikativ, aber nicht streng multiplikativ: $\mu(4) \neq \mu(2) \cdot \mu(2)$, d.h. $\mu(ab) = \mu(a)\mu(b)\ \forall a, b$ mit $(a, b) = 1$.
Es gilt : $\sum_{d|n} \mu(d) = \begin{cases} 1 & n = 1 \\ 0 & \text{sonst} \end{cases}$
Also ist $\mu * 1 = \delta$ und μ ist in $\mathcal{A}$ invertierbar mit Inversem 1.

Theorem 6.7 (Möbiussche Umkehrformel)**.** (a) Sei f eine arithmetische Funktion und sei g definiert durch $g(n) := \sum_{d|n} f(d)$, das heißt $g = f * 1$. Dann gilt $f(n) = \sum_{d|n} \mu(\frac{n}{d})\ g(d)$.

(b) Sei g eine arithmetische Funktion und sei f definiert durch $f(n) := \sum_{d|n} \mu(\frac{n}{d})\, g(d)$, das heißt $f = g * \mu$. Dann gilt $g(n) = \sum_{d|n} f(d)$.

Definition 6.8. Seien f, g reellwertige Funktionen und g positiv.

(a) $f(x) = O(g(x))$ für $x \to \infty$ ("$f(x)$ ist groß$-O$ von $g(x)$)": $\Leftrightarrow \exists$ Konstante k mit $\left|\frac{f(x)}{g(x)}\right| \leqslant k$ für x groß, d.h. $\limsup_{x\to\infty} \left|\frac{f(x)}{g(x)}\right| < \infty$.

(b) $f(x) = o(g(x))$ ("$f(x)$ ist klein$-o$ von $g(x)$"): $\Leftrightarrow \lim_{x\to\infty} \frac{f(x)}{g(x)} = 0$.

(c) $f(x) \sim g(x)$ ("$f(x)$ ist asymptotisch gleich $g(x)$) $:\Leftrightarrow \lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$.

Theorem 6.9. (a) f_1 mit $f_1(x) = \sum_{n\leqslant x} \frac{\mu(n)}{n}$ erfüllt $f_1 = O(1)$.

(b) f_2 mit $f_2(x) = \sum_{n\leqslant x} \frac{\mu(n)}{n^2}$ erfüllt $f_2 = \frac{6}{\pi^2} + O(\frac{1}{x})$.

Lemma 6.10. Sei f eine arithmetische Funktion und sei F definiert durch $F(x) := \sum_{n\leqslant x} f(n)$. Dann gilt $\sum_{m\leqslant x} F(\frac{x}{m}) = \sum_{d\leqslant x} f(d)[\frac{x}{d}] = \sum_{n\leqslant x}\sum_{d|n} f(d)$.

Proposition 6.11. Für $x \geqslant 1$ sei $\Phi(x) := \sum_{n\leqslant x} \varphi(n)$. Dann gilt: $\varphi(x) = \frac{3x^2}{\pi^2} + O(x \ln x)$

7 Teilerfunktionen

Definition 7.1. Die *Teilerfunktion* (oder *Teileranzahlfunktion*) $d : \mathbb{N} \to \mathbb{C}$ ist definiert durch $d(n) := \sharp\,\{d|n\}$.

Lemma 7.2. d ist multiplikativ.

Theorem 7.3. $\forall\ \varepsilon > 0 : d = O(n^\varepsilon)$.

Lemma 7.4. Sei f multiplikativ. Dann gilt:

(a) $f(kgV(a,b)) \cdot f(ggT\ (a,b)) = f(a)f(b)\ \forall\ a, b$.

(b) Sei $f(1) = 1$. Dann gilt: $\sum_{d|n} \mu(d)f(d) = \prod_{p|n}(1 - f(p))$.

(c) Sei $(p^k) = 2, 3, 4, 5, 7, 8, 9, 11, -$ die Folge der (aufsteigenden) Primzahlpotenzen (d.h. $n \in \mathbb{N} : \exists\ p, k, p\ prim\ mit\ n = p^k$).
Falls gilt: $\lim_{p^k\to\infty} \underbrace{f(p^k)}_{Teilfolge} = 0$, dann gilt auch: $\lim_{n\to\infty} \underbrace{f(n)}_{ganzeFolge} = 0$

Lemma 7.5. Seien f und g arithmetische Funktionen und $F(x) := \sum_{n\leqslant x} f(n)$ die Summenfunktion sowie $a, b \in \mathbb{N}_0$ mit $a < b$. Dann gilt:

(1) $\sum_{n=a+1}^{b} f(n)g(n) = F(b)g(b) - F(a)g(a+1) - \sum_{n=a+1}^{b-1} F(n)(g(n+1) - g(n))$.

(2) Sei $g(t), t \in \mathbb{R}_{\geqslant 0}$ stetig differenzierbar und seien $x, y \in \mathbb{R}_{\geqslant 0}$ mit $[y] < [x]$. Dann gilt:

$$(*) \quad \sum_{y<n\leqslant x} f(n)g(n) = F(x)g(x) - F(y)g(y) - \int_y^x F(t)g'(t)\ dt.$$

Falls $x \geqslant 2$ und g stetig differenzierbar auf $[1, x]$, dann gilt:

$$(**) \quad \sum_{n\leqslant x} f(n)g(n) = F(x)g(x) - \int_1^x F(t)g'(t)\ dt.$$

Definition 7.6. Für $t \in \mathbb{R}$ sei $t := [t] + \{t\}$ mit $[t] \in \mathbb{Z}, \{t\} \in [0, 1)$ und $[t] \leqslant t < [t] + 1$.

Die reelle Zahl $\gamma := 1 - \int_1^\infty \frac{\{t\}}{t^2}\ dt \in (0, 1)$ heißt *Euler Konstante* (oder *Euler-Mascheroni-Konstante)*.

Proposition 7.7. Für $x \in \mathbb{R}, x \geqslant 1$ gilt: $\sum_{n\leqslant x} \frac{1}{n} = ln\ x + \gamma + r(x)$, wobei $|r(x)| < \frac{1}{x}$.

Theorem 7.8.
Für $x \in \mathbb{R}_{\geqslant 1}$ und $D(x) := \sum_{n\leqslant x} d(n)$ gilt: $D(x) = x\ ln\ x + (2\gamma - 1)x + O(\sqrt{x})$.

Definition 7.9. Sei $\ell \geqslant 1$. Die arithmetische Funktion $d_\ell : \mathbb{N} \to \mathbb{C}$ ist definiert durch $d_\ell(n) := \sharp\{(d_1, \ldots, d_\ell) : n = d_1 \cdots d_\ell\}$, die Anzahl der angeordneten Faktorisierungen von n mit ℓ Faktoren. Die Summenfunktion $D_\ell : \mathbb{R} \to \mathbb{C}$ ist definiert durch $D_\ell(x) := \sum_{n\leqslant x} d_\ell(n)$.

Proposition 7.10. Sei $\ell \geqslant 1$ und $a \geqslant 1$ sowie p *prim*. Dann gilt:

(a) d_ℓ ist multiplikativ.

(b) $d_\ell(p^a) = \binom{a+\ell-1}{\ell-1}$.

Theorem 7.11. Für $\ell \geqslant 2$ gilt: $D_\ell(x) := \sum_{n\leqslant x} d_\ell(n) = \frac{1}{(\ell-1)!}\ x\ ln^{\ell-1}x + O(x\ ln^{\ell-2}x)$.

Lemma 7.12. Seien $a < b$ ganze Zahlen, $f(t) : [a, b] \to \mathbb{R}$ eine monotone Funktion. Dann gilt:

(a) $\min\{f(a), f(b)\} \leqslant \sum_{n=a}^{b} f(n) - \int_a^b f(t)\ dt \leqslant \max\{f(a), f(b)\}$.

(b) Seien $x < y$ reelle Zahlen mit $y < [x]$ und $f(t)$ nichtnegativ monoton auf $[y, x]$. Dann ist $\left| \sum_{y<n\leqslant x} f(n) - \int_y^x f(t)\ dt \right| \leqslant \max\{f(y), f(x)\}$.

(c) Sei $f(t)$ nichtnegativ auf $[1,\infty]$, monoton wachsend auf $[1,t_0]$ und monoton fallend auf $[t_0,\infty]$ für ein t_0. Dann gilt für $F(x)=\sum_{n\leqslant x} f(x) : F(x)=\int_1^x f(t)\ dt + O(1)$.

Proposition 7.13.

(a) Auf $[2,\infty]$ gilt : $\sum_{n\leqslant x} ln\ n = x\ ln\ x - x + O(ln\ x)$.

(b) Sei $r\in\mathbb{N}_0$. Auf $[1,\infty]$ gilt: $\sum_{n\leqslant x}\frac{ln^r n}{n} = \frac{1}{r+1} ln^{r+1}x + O(1)$.

(c) Sei $k\in\mathbb{N}_0$. Auf $[1,\infty]$ gilt: $\sum_{n\leqslant x}\frac{ln^k\left(\frac{x}{n}\right)}{n} = \frac{1}{k+1}\ ln^{k+1}x + O(ln^k\ x)$.

(d) Sei $k\in\mathbb{N}_0$. Dann gilt: $\sum_{n_1\cdots n_k\leqslant x}\frac{1}{n_1\cdots n_k} = \frac{1}{k!}\ ln^k x + O(ln^{k-1}\ x)$.

Proposition 7.14. $\forall\ n\in\mathbb{N} : d^2(n) = \sum_{e^2|n}\mu(e)\ d_4(\frac{n}{e^2})$.

Theorem 7.15 (Ramanujan). : $\sum_{n\leqslant x} d^2(n) \sim \frac{1}{\pi^2}\ x\ (ln\ x)^3$ (für $x\to\infty$).

8 Der Primzahlsatz

Theorem 8.1. $\Pi(x)\sim\frac{x}{ln\ x}$, d.h. $\lim\limits_{x\to\infty}\frac{\Pi(x)\ ln\ x}{x}=1$.

Definition 8.2. Die Funktionen ϑ und ψ sind definiert durch

$$\vartheta(x) := \sum_{p\leqslant x}\ln p = \ln\prod_{p\leqslant x} p \quad \text{(p prim)}.$$

$$\psi(x) := \sum_{p^k\leqslant x} ln\ p \ (p^k \text{ Primzahlpotenz}).$$

Theorem 8.3 (Chebyshev). $\exists A,B\in\mathbb{R}_{>0}\ \forall\ x\geqslant 2$:

$$Ax\leqslant\vartheta(x)\leqslant\psi(x)\leqslant\Pi(x)\ ln\ x\leqslant Bx.$$

Genauer gilt:

$$\liminf_{x\to\infty}\frac{\vartheta(x)}{x} = \liminf_{x\to\infty}\frac{\psi(x)}{x} = \liminf_{x\to\infty}\frac{\Pi(x) ln\ x}{x} \geqslant ln\ 2\sim 0,69$$

$$\limsup_{x\to\infty}\frac{\vartheta(x)}{x} = \limsup_{x\to\infty}\frac{\psi(x)}{x} = \limsup_{x\to\infty}\frac{\Pi(x) ln\ x}{x} \leqslant ln\ 4\sim 1,38$$

Korollar 8.4. $\exists\ a,b\in\mathbb{R}_{>0} : \forall\ n\geqslant 2 : a\cdot n\cdot ln\ n\leqslant p_n\leqslant b\cdot n\cdot ln\ n$.

Lemma 8.5. $\forall\ x : \psi(x)\leqslant\pi(x)\ ln\ x$.

Lemma 8.6.

(a) Sei $1 \leqslant k \leqslant n$ Dann gilt:

$$\binom{n}{k-1} < \binom{n}{k} \Leftrightarrow k < \tfrac{n+1}{2}.$$
$$\binom{n}{k-1} > \binom{n}{k} \Leftrightarrow k > \tfrac{n+1}{2}.$$
$$\binom{n}{k-1} = \binom{n}{k} \Leftrightarrow n \text{ ungerade und } k = \tfrac{n+1}{2}.$$

(b) $\forall\, n : \frac{2^{2n}}{2n} \leqslant \binom{2n}{n} < 2^{2n}$.

Proposition 8.7. $\forall n : \prod_{p \leqslant n} p < \psi^n$

$$l(n) := \begin{cases} ln\ p,\ n = p\ prim & \rightsquigarrow \vartheta(x) = \sum_{\substack{p \leqslant x \\ p\ prim}} ln\ p = \sum_{n \leqslant x} l(n) \\ 0, \text{ sonst} \end{cases}$$

$$\Lambda(n) := \begin{cases} ln\ p, n = p^k, p\ prim & \rightsquigarrow \psi(x) = \sum_{p^k \leqslant x} ln\ p = \sum_{n \leqslant x} \Lambda(n) \\ 0, \text{ sonst} \end{cases}$$

$\Lambda(n)$ ist die *von Mangoldt-Funktion* (siehe Übungsblatt 8).

Theorem 8.8 (Mertens). : $\exists$ Konstante b_1, so daß für $x \geqslant 2$ gilt:
$\sum_{p \leqslant x} \frac{1}{p} = ln\ ln\ x + b_1 + O\left(\frac{1}{ln\ x}\right)$.

Theorem 8.9 (Mertens). : $\exists$ Konstante γ, so daß für $x \geqslant 2$ gilt:
$\prod_{p \leqslant x} (1 - \frac{1}{p})^{-1} = e^{\gamma}\ ln\ x + O(1)$.

Lemma 8.10. Für $x \geqslant 2$ gilt $\sum_{m \leqslant x} \psi\left(\frac{x}{m}\right) = \sum_{d \leqslant x} \Lambda(d) \left[\frac{x}{d}\right] = x\ ln\ x - x + O(ln\ x)$.

Proposition 8.11 (Mertens). Für $x \geqslant 1$ ist

(a) $\sum_{n \leqslant x} \frac{\Lambda(n)}{n} = ln\ x + O(1)$.

(b) $\sum_{\substack{p \leqslant x \\ p\ prim}} \frac{ln\ p}{p} = ln\ x + O(1)$.

Proposition 8.12. $\sum_{n \leqslant x} \frac{\vartheta(n)}{n^2} = ln\ x + O(1)$.

Theorem 8.13 (Hardy-Ramanujan). Sei $\delta > 0$. Dann gilt:

$$\sharp\{n \leqslant x : |\omega(n) - ln\ ln\ n| \geqslant (ln\ ln\ x)^{\frac{1}{2}+\delta}\} = o(x).$$

Proposition 8.14. Für $x \geqslant 2$ gilt:

(a) $\sum_{n \leqslant x} \omega(n) = x \ln \ln x + b_1 x + O\left(\frac{x}{\ln x}\right)$. (für b_1 aus 8.8, Satz von Mertens)

(b) $\sum_{n \leqslant x} \omega(n)^2 = x(\ln \ln x)^2 + O(x \ln \ln x)$.

Lemma 8.15 (Chebyshev Ungleichung)**.** Sei $S \subset \mathbb{Z}, |S| < \infty, f : S \to \mathbb{R}, \mu \in \mathbb{R}, t \in \mathbb{R}_{>0}$. Dann gilt:

$$\sharp\{n \in S : |f(n) - \mu| \geqslant t\} \leqslant \tfrac{1}{t^2} \sum_{n \in S} (f(n) - \mu)^2.$$

Definition 8.16. Für $r \in \mathbb{N}_0$ ist die *verallgemeinerte von Mangoldt-Funktion* Λ_r definiert durch $\Lambda_r := \mu * L^r$.

Lemma 8.17. $\forall\ n \in \mathbb{N} : \Lambda_2(n) = \Lambda(n) ln\ n + (\Lambda * \Lambda)(n)$.

Theorem 8.18 (Selbergs Formel)**.** : Sei $x \geqslant 1$ Dann gilt:

(a) $\sum_{n \leqslant x} \Lambda_2(n) = 2x\ ln\ x + O(x)$.

(b) $\sum_{p \leqslant x} ln^2 p + \sum_{pq \leqslant x} ln\ p\ ln\ q = 2\ x\ ln\ x\ + O(x)$.

(c) $\vartheta(x)\ ln\ x + \sum_{p \leqslant\ x} ln\ p\ \vartheta\left(\frac{x}{p}\right) = 2\ x\ ln\ x + O(x)$.

(d) $\sum_{p \leqslant x} ln\ p + \sum_{pq \leqslant x} \frac{ln\ p\ ln\ q}{ln\ pq} = 2\ x + O\left(\frac{x}{1 + ln\ x}\right)$.

Proposition 8.19. Für $x \geqslant 1$ gilt: $|R(x)| \leqslant \frac{1}{ln\ x} \sum_{n \leqslant x} |R\left(\frac{x}{n}\right)| + \underbrace{O\left(\frac{x\ ln\ ln\ x}{ln\ x}\right)}_{=O(x)}$.

Lemma 8.20. Für $x > e$ ist $\sum_{\substack{p \leqslant x \\ p\ prim}} \frac{ln\ p}{p\left(1 + ln \frac{x}{p}\right)} = O(ln\ ln\ x)$.

Lemma 8.21.
$\exists c_0 \geqslant 1\ \forall \delta \in (0,1)\ \exists\ x_1(\delta) \geqslant 4 : \forall\ x \geqslant x_1(\delta)\ \exists\ n \in [x, e^{c_0/\delta} x] : |R(n)| < \delta_n$.

Lemma 8.22. Sei c_0 wie in 8.21 und $0 < \delta < 1$ Dann $\exists\ x_2(\delta)$,
so daß $\forall\ x \geqslant x_2(\delta)\ \exists\ y : (x, e^{c_0/\delta} x] \supset (y, e^{\delta/2} y]$.
so daß $\forall\ t \in (y, e^{\delta/2} y] : |R(t)| < 4\delta t$.

Theorem 8.23 (äquivalent zum Primzahlsatz)**.** $\vartheta(x) \underset{x \to \infty}{\sim} x$