# 0. Grundbegriffe

**0.1. Teilbarkeit in $\mathbb{N}$.** Mit $\mathbb{N}_1$ (oder auch nur $\mathbb{N}$, zumindest in dieser Vorlesung) werde die Menge $\{1, 2, \dots\}$ der ganzen Zahlen $n \geq 1$ bezeichnet; wir nennen diese Zahlen die *natürlichen* Zahlen.

Wir verwenden das Induktionsprinzip: *Jede nicht leere Teilmenge von $\mathbb{N}$ besitzt ein kleinstes Element* (und dieses ist eindeutig bestimmt!).

**Teiler.** Seien $a, b$ natürliche Zahlen. Man sagt $a$ teilt $b$, falls es eine natürliche Zahl $a'$ mit $aa' = b$ gibt; man nennt dann $a$ einen *Teiler* von $b$ und man schreibt $a|b$.

**Wichtig.** Die Zahl 1 besitzt nur einen Teiler, nämlich sich selbst.

Man nennt die natürlichen Zahlen $a, b$ *teilerfremd,* wenn 1 der einzige gemeinsame Teiler ist.

**Primzahl.** Eine natürliche Zahl $p$ heißt *Primzahl,* wenn $p > 1$ gilt und $1, p$ die einzigen Teiler von $p$ sind.

**Wichtig.** *Sei $n > 1$ eine natürliche Zahl. Der kleinste von 1 verschiedene Teiler von $n$ ist eine Primzahl.* (Der "kleinste" Teiler von $n$ existiert nach dem Induktionsprinzip.)

**Fundamentalsatz der elementaren Zahlentheore:** Zu jeder natürlichen Zahl $n$ gibt es Primzahlen $p_1 \leq p_2 \leq \cdots \leq p_t$ mit $n = p_1 p_2 \cdots p_t$, und *diese Zahlenfolge ist eindeutig.*

Dieser Satz ist **keinesfalls trivial** und auch **gar nicht offensichtlich,** auch wenn man sich durch den Schulunterricht an ihn gewöhnt hat! Ein Beweis wird üblicherweise in der Vorlesung *Lineare Algebra* gegeben. Später soll dies auch in dieser Vorlesung thematisiert werden. Jetzt wird der Satz als bekannt vorausgesetzt.

Ist $n$ eine natürliche Zahl und $p$ Primzahl, so sei $n_p$ die höchste $p$-Potenz, die $n$ teilt. *Es gilt* $n = \prod_p n_p$. Ist $n_p = p^s$, so schreibt man auch $w_p(n) = s$. Man nennt $w_p$ die $p$-adische Bewertung. Es gilt also $n = \prod_p p^{w_p(n)}$.

Beispiele: $12_2 = 4,\ 12_3 = 3,\ 12_5 = 1.$
$w_2(12) = 2,\ w_3(12) = 1,\ w_5(12) = 0.$

Konventionen: $p$ steht üblicherweise für eine Primzahl; bei einer Reihe der Form $\sum_p f(p)$ wird über alle Primzahlen $p$ summiert, entsprechend steht $\prod_p f(p)$ dafür, dass das Produkt der Werte $f(p)$ über alle Primzahlen $p$ zu bilden ist.

**0.2. Der ganzzahlige Anteil einer reellen Zahl.** Mit $\mathbb{Z}$ bezeichnen wir den *Ring der ganzen Zahlen.* Ist $x$ eine reelle Zahl, so sei $\lfloor x \rfloor$ die größte ganze Zahl, die kleiner oder gleich $x$ ist. Also: $\lfloor x \rfloor$ ist diejenige ganze Zahl $z$ mit $z \leq x < z + 1$.

**Lemma.**

$$\lfloor x\rfloor + \lfloor y\rfloor \le \lfloor x+y\rfloor \le \lfloor x\rfloor + \lfloor y\rfloor + 1 \qquad \text{für alle} \qquad x, y \in \mathbb{R}.$$

Beweis: $\lfloor x\rfloor \le x$ und $\lfloor y\rfloor \le y$ impliziert $\lfloor x\rfloor + \lfloor y\rfloor \le x+y$ und damit die linke Ungleichung. Und es ist $x + y < \lfloor x\rfloor + 1 + \lfloor x\rfloor + 1$; rechts steht eine ganze Zahl $z$, die echt größer als $x+y$ ist; demnach ist $\lfloor x+y\rfloor \le z-1$; dies liefert die zweite Ungleichung.

Umformulierung:

$$0 \le \lfloor x+y\rfloor - \lfloor x\rfloor - \lfloor y\rfloor \le 1 \qquad \text{für alle} \qquad x, y \in \mathbb{R}.$$

# 1. Die Verteilung der Primzahlen.

## 1.1. Es gibt unendlich viele Primzahlen.

**Satz (Euklid).** *Es gibt unendlich viele Primzahlen.*

Wir werden viele Beweise dafür notieren; einige dieser Beweise werden Übungsaufgaben oder Präsenzaufgaben sein.

**1. Beweis (Euklid).** Seien $p_1, \ldots, p_t$ paarweise verschiedene Primzahlen mit $t \ge 1$. Bilde $n = \prod_i p_i + 1$. Sei $a$ der kleinste von 1 verschiedene Teiler von $n$. Dies ist eine Primzahl. Wäre $a = p_i$ für ein $1 \le i \le i$, etwa $a = p_1$, und $n = aa'$, so wäre $1 = n - \prod_i p_i = p_1(a' - \prod_{i\ge 2} p_i)$, also $p_1$ ein Teiler von 1. (Dieser Beweis gibt ein Verfahren an, wie man zu einer vorgegebenen endlichen Menge von Primzahlen weitere Primzahlen konstruieren kann.)

**2. Beweis.** *Zu jeder natürlichen Zahl $n > 2$ gibt es eine Primzahl $p$ mit $n < p < n!$.* (Eine der Präsenzaufgaben; hier wird ein Zahlenintervall genannt, in dem auf jeden Fall mindestens eine Primzahl liegen muss.)

**5. Beweis.** *Sei $n$ eine natürliche Zahl. Behauptung: die Zahlen $1 + d \cdot n!$ mit $1 \le d \le n$ sind größer als 1 und paarweise teilerfremd.* Beweis: Betrachte zwei verschiedene solche Zahlen, etwa $1 + d \cdot n!$ und $1 + d' \cdot n!$ mit $1 \le d < d' \le n$. Sei $p$ ein gemeinsamer Primteiler dieser beiden Zahlen, dann ist $p$ auch ein Teiler der Differenz: $p|(d' - d) \cdot n!$. Wegen $1 \le d' - d \le n$ ist dann $p$ auch ein Teiler von $n!$ und demnach von $d \cdot n!$. Da $p$ ein Teiler von $1 + d \cdot n!$ und von $d \cdot n!$ ist, folgt $p|1$. Widerspruch. (Da der Beweis $n$ Zahlen größer als 1 liefert, die paarweise teilerfremd sind, sehen wir: es gibt mindestens $n$ verschiedene Primzahlen — man nehme je einen Primteiler dieser Zahlen.)

**7. Beweis (Euler).** Sind $p_1, \ldots, p_t$ paarweise verschiedene Primzahlen, so sei $\mathcal{Z}(p_1, \ldots, p_t)$ die Menge der natürlichen Zahlen, in deren Primfaktorzerlegung nur die Primzahlen $p_1, \ldots, p_t$ auftreten (mit beliebigen Multiplizitäten).

Sei $p$ eine Primzahl. Wegen $p \geq 2$ konvergiert die geometrische Reihe $\sum_{j=0}^{\infty}(\frac{1}{p})^j$ (genauer: es ist $\sum_{j=0}^{\infty}(\frac{1}{p})^j = \frac{p}{p-1} = \frac{1}{1-p^{-1}}$). Betrachten wir $t$ paarweise verschiedenen Primzahlen $p_1, \ldots, p_t$, so gilt demnach

$$\prod_{i=1}^{t} \sum_{j=0}^{\infty} (\frac{1}{p_i})^j = \prod_{i=1}^{t} \frac{p_i}{p_i - 1}.$$

Diese geometrischen Reihen haben positive Summanden, sind also absolut konvergent, das Produkt der geometrischen Reihen kann durch gliedweises Ausmultiplizieren berechnet werden. Die einzelnen Summanden links haben die Form

$$(\frac{1}{p_1})^{j_1}(\frac{1}{p_2})^{j_2} \cdots (\frac{1}{p_t})^{j_t} = \frac{1}{n} \qquad \text{mit} \qquad n = (p_1)^{j_1}(p_2)^{j_2} \cdots (p_t)^{j_t},$$

Wir sehen: links steht die Summe der Zahlen $\frac{1}{n}$, mit $n \in \mathcal{Z}(p_1, \ldots, p_t)$, jede derartige Zahl $\frac{1}{n}$ kommt genau einmal vor.

Es folgt, dass $\mathcal{Z}(p_1, \ldots, p_t)$ eine echte Teilmenge von $\mathbb{N}$ sein muss, denn die harmonische Reihe $\sum_{n\in\mathbb{N}} \frac{1}{n}$ ist bekanntlich divergent.

Man kann mit einem ähnlichen Beweis auch folgendes zeigen:

**Satz.** *Die Reihe $\sum_p \frac{1}{p}$ divergiert.*

Vorbemerkung: Man nennt eine natürliche Zahl $n$ eine *Quadratzahl,* falls es $m \in \mathbb{N}$ gibt mit $n = m^2$, man nennt $n$ *quadratfrei*, falls $m^2|n$ nur für $m = 1$ gilt. Man sieht sofort: Ist $n = p_1^{e_1}p_2^{e_2}\cdots p_t^{e_t}$ mit Primzahlen $p_1 < p_2 < \cdots < p_t$, so ist $n$ genau dann eine Quadratzahl, wenn alle Exponenten $e_i$ gerade sind, und quadratfrei, wenn alle Exponenten Null oder Eins sind. Die einzige natürliche Zahl $n$, die sowohl eine Quadratzahl, also auch quadratfrei ist, ist $n = 1$. Und es gilt: Jede natürliche Zahl $n$ lässt sich **eindeutig** als Produkt einer Quadratzahl und einer quadratfreien Zahl schreiben.

Nun zum Beweis des Satzes. Angenommen, $\sum_p \frac{1}{p} = \beta \in \mathbb{R}$. Für jede natürliche Zahl $n$ sei $Q(n)$ die Menge der quadratfreien Zahlen $m < n$, und $Q$ die Menge aller quadratfreien natürlichen Zahlen. Jede Zahl in $Q(m)$ läßt sich als Produkt von Primzahlen $p < n$ schreiben, daher ist

$$\sum_{m\in Q(n)} \frac{1}{m} \;\leq\; \prod_{p<n} (1 + \frac{1}{p})$$

Für jede Zahl $x > 0$ gilt $1 + x < \exp(x)$ (wegen der Reihenentwicklung von exp), also ist

$$\prod_{p<n} (1 + \frac{1}{p}) < \prod_{p<n} \exp(\frac{1}{p}) = \exp(\sum_{p<n} \frac{1}{p}) \leq \exp(\beta).$$

Dies zeigt, dass die Reihe $\sum_{m\in Q} \frac{1}{m}$ konvergiert, da die Partialsummen $\sum_{m\in Q(n)} \frac{1}{m}$ beschränkt sind.

Bekanntlich konvergiert auch $\sum_{n\in\mathbb{N}} \frac{1}{n^2}$. Es ist aber

$$(\sum_{n\in\mathbb{N}} \frac{1}{n^2})(\sum_{m\in Q} \frac{1}{m})$$

die harmonische Reihe, und die harmonische Reihe konvergiert nicht! Dieser Widerspruch zeigt, dass die Reige $\sum_p \frac{1}{p}$ divergent sein muss.

Bemerkung. Da die Reihe $\sum_n \frac{1}{n^2}$ konvergiert, während die Reihen $\sum_p \frac{1}{p}$ und $\sum_{m\in Q} \frac{1}{m}$ divergieren, sagt man manchmal: *es gibt viel mehr Primzahlen und erst recht viel mehr quadratfreie Zahlen als Quadratzahlen.*

**8. Beweis: Das Bertrand'sche Postulat.** Siehe Abschnitt 1.3.

Und viele weitere! (siehe die weitere Vorlesung, aber auch die Übungsaufgaben und die Präsenz-Aufgaben; insbesondere findet man dort die hier übersprungenen Beweise 3, 4 und 6).

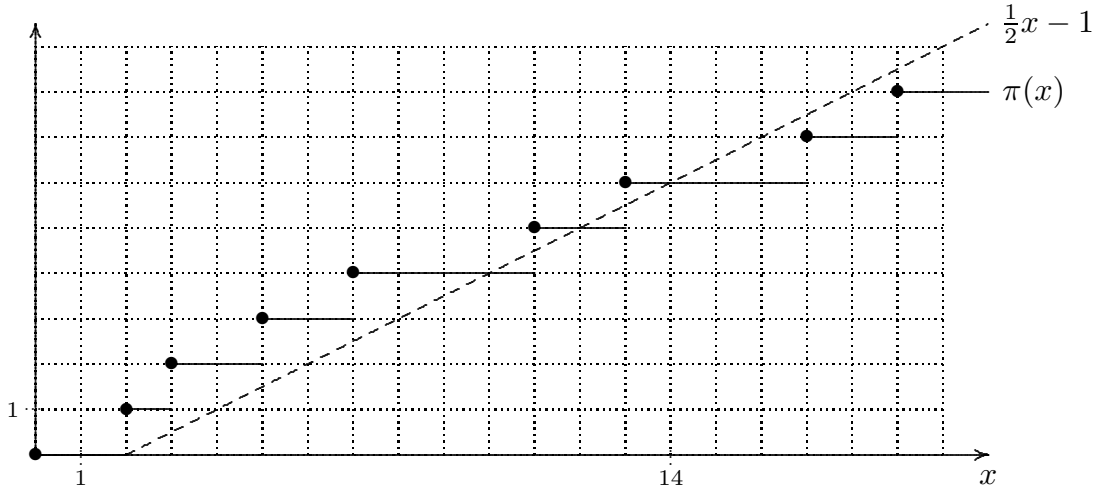
### 1.2. Die Funktion $\pi(x)$.

Ist $x$ eine reelle Zahl, so sei $\pi(x)$ die *Anzahl der Primzahlen* $p \le x$.

Beispiele: $\pi(5) = 3,\ \pi(\frac{5}{2}) = 1,\ \pi(-2) = 0.$

**Lemma.** $\pi(x) \le \frac{1}{2}x - 1$ für $x \ge 14$.

Beweis: Bis auf die Zahl 2 sind alle Primzahlen ungerade. Die Behauptung ist richtig für $x = 14$ und $x = 15$ (die Primzahlen $p \le 15$ sind $2, 3, 5, 7, 11, 13$, es ist also $\pi(14) = \pi(15) = 6 = \frac{14}{2} - 1 < \frac{15}{2} - 1$). Ist die Behauptung richtig für eine ungerade Zahl $x$ größer als 2, so für alle Zahlen $y$ mit $x \le y$ (und 15 ist die kleinste ungerade ganze Zahl $y$, für die die Behauptung richtig ist).



### 1.3. Das Bertrand'sche Postulat.

**Satz (Tchebycheff) ("Bertrand'sches Postulat").** *Zu jeder natürlichen Zahl $n$ gibt es eine Primzahl $p$ mit $n < p \leq 2n$.*

Der Fall $p = 2n$ kann natürlich nur für $n = 1$ auftreten, also: *Zu jeder natürlichen Zahl $n > 1$ gibt es eine Primzahl $p$ mit $n < p < 2n$.*

Natürlich ist dieser Satz von Tchebycheff ein weiterer Beweis des Euklid'schen Satzes. Vermutet wurde die Aussage 1845 von Bertrand, bewiesen wurde sie 1852 von Tchebycheff. Der folgende Beweis stammt im wesentlichen von Erdös.

Der allgemeine Beweis, der hier vorgestellt wird, funktioniert nicht für kleine Zahlen $n$, sondern nur für $n \geq 365$.

Für $n \leq 364$ betrachtet man die folgende Primzahlfolge

$$2,\ 3,\ 5,\ 7,\ 13,\ 23,\ 43,\ 83,\ 163,\ 317,\ 631.$$

Für diese Primzahlen $p_1 < \cdots < p_{11}$ gilt: $p_{i+1} < 2p_i$, für $1 \leq i \leq 10$. Also gibt es zu jeder Zahl $n \leq 364$ eine der Zahlen $p_i$ mit $n < p_i \leq 2n$. (Für $n = 1$ nimmt man $p_1 = 2$, ist $p_{i-1} \leq n < p_i$, so nimmt man $p_i$, denn $n < p_i < 2p_{i-1} \leq 2n$.)

Die **Hauptidee** für den allgemeinen Beweis: Man betrachtet den Binomialkoeffizienten $\binom{2n}{n} = \frac{(2n)!}{n!n!}$, denn alle Primzahlen $p$ mit $n < p \leq 2n$ sind Teiler des Zählers, aber nicht des Nenners, also Teiler von $\binom{2n}{n}$; für $n < p \leq 2n$ ist $p$ ein Teiler von $\binom{2n}{n}$, und offensichtlich ist $p^2$ kein Teiler von $\binom{2n}{n}$. Wir sehen also: Ist $n < p \leq 2n$, so ist $\binom{2n}{n}_p = p$.

Für die Primteiler von $\binom{2n}{n}$ gelten weitere Eigenschaften, zum Beispiel: Alle Primfaktoren $p$ von $\binom{2n}{n}$ erfüllen $p \leq 2n$; dies ist ein Spezialfall der folgenden Behauptung (3). Hier sind die wesentlichen Behauptungen, die wir brauchen:

**(1)** Ist $n < p \leq 2n$, so ist $\binom{2n}{n}_p = p$.

**(2)** Ist $\frac{2}{3}n < p \leq n$, und $p \geq 3$, so ist $\binom{2n}{n}_p = 1$ (das heißt: $p$ ist kein Teiler von $\binom{2n}{n}$), dies ist eine wesentliche Einsicht von Erdös.

**(3)** Für alle Primzahlen $p$ gilt: $\binom{2n}{n}_p \leq 2n$.

(3′) Daraus folgt: Ist $\sqrt{2n} < p$, so ist $p^2$ kein Teiler von $\binom{2n}{n}$.

Und wir brauchen zwei zusätzliche Abschätzungen:

**(4)** $\frac{1}{2n}4^n \leq \binom{2n}{n}$.

**(5)** $\prod_{p \leq x} \leq 4^{x-1}$ für jede natürliche Zahl $x$.

Beweise:

(1) Dies wurde schon notiert.

(2) Wieder verwenden wir $\binom{2n}{n} = \frac{(2n)!}{n!n!}$. Aus $\frac{2}{3}n < p \leq n$ folgt, dass $p$ genau zweimal den Zähler teilt und genau einmal jeden der beiden Faktoren $n!$ im Nenner. Also heben sich die Faktoren $p$ in Zähler und Nenner weg.

(3) Hier müssen wir weiter ausholen. Wir brauchen folgende Formel von Legendre:

**Lemma (Legendre).**

$$\boxed{w_p(n!) = \lfloor n/p \rfloor + \lfloor n/p^2 \rfloor + \cdots}$$

Beweis: Die Anzahl der Faktoren von $n! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n$, die durch $p$ teilbar sind, ist $\lfloor n/p \rfloor$, die Anzahl der Faktoren, die durch $p^2$ teilbar sind, ist $\lfloor n/p^2 \rfloor$, usw.

Die Legendre-Formel hat viele Anwendungen. Zum Beispiel: Wieviele Nullen hat die Dezimaldarstellung von 100! am Ende? Gesucht ist also $w_2(100!)$ und $w_5(100!)$. Es ist

$$w_2(100!) = 50 + 25 + 12 + 6 + 3 + 1 = 97$$
$$w_5(100!) = 20 + 4 = 24$$

Die Anzahl der Endnullen von 100! ist das Minimum von 97 und 24, also 24.

Beweis von (3): Sei $s$ maximal mit $p^s \leq 2n$. Nach der Legendre-Formel ist

$$a := w_p(\tbinom{2n}{n}) = \sum_{t \geq 1} (\lfloor 2n/p^t \rfloor - 2\lfloor n/p^t \rfloor),$$

dabei wird über alle $t$ summiert, für die $p^t \leq 2n$ gilt, also über $1 \leq t \leq s$. Für jeden Summanden gilt

$$0 \leq \lfloor 2n/p^t \rfloor - 2\lfloor n/p^t \rfloor \leq 1$$

(siehe den Abschnitt "Grundbegriffe"). Wir sehen also: Es gibt genau $s$ Summanden und alle Summanden sind 0 oder 1, also gilt $a \leq s$. Die höchste $p$-Potenz, die $\binom{2n}{n}$ teilt, ist $p^a$, und es ist $p^a \leq p^s \leq 2n$.

(3′) Sei $\sqrt{2n} < p$. Dann ist $2n < p^2$. Wäre $p^2$ ein Teiler von $\binom{2n}{n}$, so wäre $p^2 \leq 2n$ nach (3), ein Widerspruch.

(4) Wir zeigen als erstes: Ist $k < \frac{m-1}{2}$, also $k + 1 < m - k$, so ist

$$\binom{m}{k} = \frac{m!}{k!(m-k)!} < \frac{m-k}{k+1} \cdot \frac{m!}{k!(m-k)!} = \frac{m!}{(k+1)!(m-k-1)!} = \binom{m}{k+1}.$$

Demnach liefern die Binomialkoeffizienten eine Folge von Zahlen, die zur Mitte hin ansteigt und dann wieder abfällt:

$$1 = \tbinom{2n}{0} < \tbinom{2n}{1} < \cdots < \tbinom{2n}{n} > \cdots > \tbinom{2n}{2n-1} > \tbinom{2n}{2n} = 1,$$

Wir betrachten die folgende Summe mit $2n$ Summanden:

$$(1+1)^{2n} = \left(\binom{2n}{0} + \binom{2n}{2n}\right) + \binom{2n}{1} + \binom{2n}{2} + \cdots + \binom{2n}{n-1}$$

Für jeden Summanden $s_i$ gilt $s_i \leq \binom{2n}{n}$. Also ist

$$2^{2n} = \sum_i s_i \leq 2n \cdot \binom{2n}{n},$$

und damit ist (4) bewiesen.

(5) Setze $P(x) = \prod_{p \leq x} p$. Ist $q$ die größte Primzahl mit $q \leq x$, so ist $P(q) = P(x)$ and $4^{q-1} \leq 4^{x-1}$. Also reicht es, den Fall $x = q$ zu untersuchen. Ist $q = 2$, so ist $P(q) = 2 < 4 = 4^{2-1}$. Sei nun $q = 2m+1$ eine ungerade Primzahl. Es ist

$$\prod_{m+1 < p \leq 2m+1} p \leq \binom{2m+1}{m} \leq 2^{2m} = 4^m.$$

Die erste Ungleichung gilt aus dem gleichen Grund wie die Behauptung (1). Für die zweite argumentiert man wie folgt: Die beiden Binomialkoeffizieten $\binom{2m+1}{m}$ und $\binom{2m+1}{m+1}$ sind gleich, es ist also

$$2\binom{2m+1}{m} = \binom{2m+1}{m} + \binom{2m+1}{m+1} \leq \sum_{k=0}^{2m+1} \binom{2m+1}{k} = (1+1)^{2m+1} = 2^{2m+1},$$

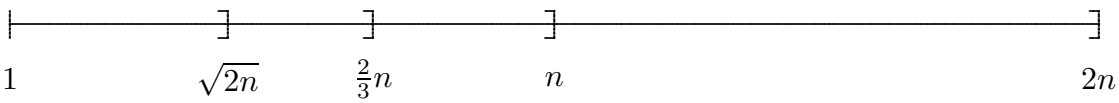
und demnach $\binom{2m+1}{m} \leq 2^{2m}$.

Also ist

$$P(q) = P(m+1) \cdot \prod_{m+1 < p \leq 2m+1} p \leq 4^m \cdot 4^m = 4^{2m}.$$

Hier verwenden wir einerseits Induktion, andererseits die gerade bewiesene Formel.

Hier nun also der **Beweis** des Bertrand'schen Postulats. Sei $n \geq 5$, dann ist $\sqrt{2n} < \frac{2}{3}n$. Die Primteiler von $\binom{2n}{n}$ sind Zahlen im Intervall $[1, 2n]$; wir betrachten verschiedene Teilintervalle:




Wegen (4) und (3) gilt:

$$\frac{4^n}{2n} \leq \binom{2n}{n} = \prod_{p \leq 2n} \binom{2n}{n}_p = a \cdot b \cdot c \cdot d$$

mit

$$a = \prod_{p \le \sqrt{2n}} \binom{2n}{n}_p \le \prod_{p \le \sqrt{2n}} 2n \;=\; (2n)^{\pi(\sqrt{2n})} \;\le\; (2n)^{\frac{1}{2}\sqrt{2n}-1},$$

$$b = \prod_{\sqrt{2n} < p \le \frac{2}{3}n} \binom{2n}{n}_p \le \prod_{\sqrt{2n} < p \le \frac{2}{3}n} p \le \prod_{p \le \frac{2}{3}n} p \;\le\; 4^{\frac{2}{3}n-1} < 4^{\frac{2}{3}n},$$

$$c = \prod_{\frac{2}{3}n < p \le n} \binom{2n}{n}_p = 1,$$

$$d = \prod_{n < p \le 2n} \binom{2n}{n}_p,$$

dabei gilt die letzte Ungleichung bei $a$ zumindest für $\sqrt{2n} \ge 14$, also $2n \ge 196$, also $n \ge 98$ (wir verwenden hier $\pi(x) \le \frac{1}{2}x - 1$, siehe Abschnitt 1.2); zusätzlich haben wir für $a$ auch (3) verwendet. Für $b$ braucht man (3′) und (5), und (c) folgt aus (2).

Dies sind die entscheidenden Abschätzungen!.

Wäre nun $d = 1$, so erhalten wir

$$\frac{4^n}{2n} \le \binom{2n}{n} \le\; a \cdot b \;\le\; (2n)^{\frac{1}{2}\sqrt{2n}-1} \cdot 4^{\frac{2}{3}n},$$

also

$$\boxed{4^{\frac{1}{3}n} \le (2n)^{\frac{1}{2}\sqrt{2n}}.}$$

Eine solche Ungleichung kann nur für kleine $n$ erfüllt sein! Zum Beispiel ist sie schon für $n = 72$ falsch (links steht: $4^{24}$, rechts steht $144^{\frac{1}{2}\sqrt{144}} = 144^6$. Es ist $4^4 = 256$. Wegen $256 > 144$ ist auch $256^6 > 144^6$).

Wir behaupten, dass die Ungleichung impliziert, dass $n \le 364$ gilt. Denn wir erhalten als dritte Potenz

$$(*) \qquad 2^{2n} = 4^n \le (2n)^{\frac{3}{2}\sqrt{2n}} \le 2^{6\,\sqrt[6]{2n}\frac{3}{2}\sqrt{2n}} = 2^{9(2n)^{2/3}}.$$

Hier verwenden wir

$$2n \le 2^{6\,\sqrt[6]{2n}}$$

Beweis: Es ist leicht zu sehen, dass $x + 1 \le 2^x$ für alle $x \ge 1$ gilt. Wir verwenden dies für $x = \sqrt[6]{2n}$ und erhalten:

$$2n = (\sqrt[6]{2n})^6 < (\sqrt[6]{2n} + 1)^6 \le (2^{\sqrt[6]{2n}})^6 = 2^{6\,\sqrt[6]{2n}}.$$

Exponentenvergleich in $(*)$ liefert

$$2n \le 9(2n)^{2/3},$$

also

$$(2n)^{1/3} \leq 9,$$

also

$$2n \leq 729, \qquad \text{also} \qquad n \leq 364.$$

### 1.4. Folgerungen aus dem Satz von Tchebycheff.

**1.4.1.** *Ist $n \geq 2$ eine natürliche Zahl, so gibt es eine Primzahl $p$ mit $n < p < 2n$.*

Beweis: Der Fall $p = 2n$ kann nur für $n = 1$ auftreten.

**1.4.2.** *Sei $n \geq 2$. Es gibt mindestens eine Primzahl $p$ mit $(n!)_p = p$.*

Beweis: Für $n = 2$ nimmt man $p = 2$. Ist $n = 2m$, mit $m \geq 2$, so nimmt man eine Primzahl $p$ mit $m < p \leq 2m = n$, offensichtlich tritt $p$ in der Primfaktorzerlegung von $n!$ mit der Vielfachheit 1 auf. Ist $n = 2m+1$, so gibt es eine Primzahl $p$ mit $m < p \leq 2m$. Es ist also $p < 2m + 1 = n$. Da $2p$ eine gerade Zahl ist, folgt aus $2p > 2m$, dass gilt $2p > 2m + 1 = n$. Daher gilt wieder, dass $p$ in der Primfaktorzerlegung von $n!$ mit der Vielfachheit 1 auftritt.

**1.4.3.** *Ist $n!$ eine $t$-Potenz, so ist $t = 1$.* (Dabei nennt man eine natürliche Zahl $m$ eine $t$-te Potenz ($t \in \mathbb{N}$), falls es eine natürliche Zahl $k$ mit $m = k^t$ gibt.)

Beweis: In der Primfaktorzerlegung einer $t$-ten Potent sind alle Exponenten Vielfache von $t$.

Sei $p_k$ die $k$-te Primzahl, also $p_1 = 2,\ p_2 = 3$, usw.

**1.4.4.**

$$\boxed{p_{n+1} < 2 \cdot p_n.}$$

Nach 1.4.1 gibt es zu $p_n \geq 2$ eine Primzahl $p$ mit $p_n < p < 2p_{n+1}$.

### 1.5. Vergleich von $\pi(x)$ mit $x/\ln x$

Die Funktion $\pi(x)$ spielt eine wichtige Rolle in der Zahlentheorie, allerdings ist dies eine Treppenfunktion, also nicht einmal eine stetige Funktion. Man versucht, diese Funktion zu anderen, schöneren (insbesondere stetigen) Funktionen in Beziehung zu setzen, insbesondere betrachtet man skalare Vielfache der Funktion $x/\ln(x)$.

**Satz.** Es gibt positive reelle Zahlen $a < 1 < b$ mit

$$\boxed{a\frac{x}{\ln x} \ \leq \ \pi(x) \ \leq \ b\frac{x}{\ln x} \qquad \text{für} \qquad x \geq 2,}$$

zum Beispiel $a = \frac{\ln 2}{4}, \quad b = 6 \ln 2$.

Zum Beweis verwenden wir wieder die Aussagen in 1.3 zu $\binom{2n}{n}$.

Es gilt:

$$n^{\pi(2n)-\pi(n)} = \prod_{n<p\le 2n} n \le \prod_{n<p\le 2n} p \le \binom{2n}{n} = \prod_{p\le 2n} \binom{2n}{n}_p \le \prod_{p\le 2n} 2n = (2n)^{\pi(2n)}.$$

Dabei ist das erste Vergleichszeichen trivial, das zweite ist die Aussage (1), das dritte ist die Aussage (3).

Wir haben aber auch die Ungleichungen

$$2^n \le \binom{2n}{n} \le 2^{2n}.$$

(In (4) wurde $\binom{2n}{n}$ nach unten durch $\frac{2^n 2^n}{2n}$ abgeschätzt, aber $2n \le 2^n$, dies zeigt die untere Abschätzung. Die obere ist ebenfalls wohlbekannt: die Summe der Binomialkoeffizienten $\binom{2n}{k}$ ist $(1+1)^{2n} = 2^{2n}$.

Insgesamt erhalten wir die beiden linken Abschätzungen:

(a) $$n^{\pi(2n)-\pi(n)} \le \binom{2n}{n} \le 2^{2n}, \qquad \text{also} \qquad \pi(2n) - \pi(n) \le \frac{2n \ln 2}{\ln n}$$

(b) $$2^n \le \binom{2n}{n} \le (2n)^{\pi(2n)}, \qquad \text{also} \qquad \frac{n \ln 2}{\ln(2n)} \le \pi(2n).$$

die rechten ergeben sich durch Logarithmieren.

Wir verwenden nun die Abschätzung (b), um $\pi(x)$ nach unten abzuschätzen: Sei $2n$ die größte ganze Zahl mit $2n \le x$. Dann sehen wir:

$$\pi(x) \ge \pi(2n) \ge \frac{n \ln 2}{\ln(2n)} \ge \frac{n \ln 2}{\ln(x)} \ge \frac{2n+2}{4} \cdot \frac{\ln 2}{\ln x} \ge \frac{\ln 2}{4} \cdot \frac{x}{\ln x};$$

dabei verwenden wir, dass gilt $n \ge \frac{2n+2}{4}$ und $2n + 2 > x$.

Jetzt wenden wir uns der Aufgabe zu, $\pi(x)$ nach oben abzuschätzen. Wir zeigen, dass aus (a) die Ungleichung

$$\pi(2^t) \le 3 \cdot \frac{2^t}{t} \qquad \text{für} \qquad t \in \mathbb{N}$$

folgt. Für $t \le 5$ wird dies direkt verifiziert:

| $t$ | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| $3\frac{2^t}{t}$ | 6 | 6 | 8 | 12 | $\frac{96}{5}$ |
| $\pi(2^t)$ | 1 | 2 | 4 | 6 | 11 |

Für $t \geq 5$ arbeitet man mit Induktion. Die Ungleichung (a) besagt für $n = 2^t$:

$$\pi(2^{t+1}) - \pi(2^t) \leq \frac{2 \cdot 2^t \cdot \ln 2}{\ln 2^t} = \frac{2^{t+1}}{t},$$

also ist

$$\pi(2^{t+1}) \leq \pi(2^t) + \frac{2^{t+1}}{t} \leq \frac{3 \cdot 2^t}{t} + \frac{2 \cdot 2^t}{t} = \frac{5 \cdot 2^t}{t} \leq \frac{3 \cdot 2^{t+1}}{t+1}$$

dabei gilt die letzte Abschätzung wegen $\frac{5}{t} \leq \frac{6}{t+1}$ (hier verwendet man $5 \leq t$).

Sei nun $2^t \leq x \leq 2^{t+1}$. Dann gilt (Zähler-Vergleich, Nenner-Vergleich):

$$\frac{2^t}{\ln 2^{t+1}} \ \leq \ \frac{x}{\ln x},$$

also

$$\pi(x) \leq \pi(2^{t+1}) \leq \frac{3 \cdot 2^{t+1}}{t+1} = 6\frac{1}{t+1}2^t \ = \ 6\frac{\ln 2}{\ln 2^{t+1}}2^t \ \leq \ 6 \ln 2 \frac{x}{\ln x}$$

**1.6. Folgerung.**

$$\pi(n^2) \geq n \qquad \text{für} \qquad n \geq 2.$$

Beweis: Für $n \leq 63$ lässt sich die Ungleichung direkt zeigen: Man braucht dafür nur die folgenden Werte

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| $n$ | = | 1 | 2 | 3 | 5 | 10 | 18 |
| $\pi(n^2)$ | = | 0 | 2 | 4 | 9 | 25 | 66 |

Sei also $n \geq 64$. Es ist

$$\pi(n^2) \geq \frac{\ln 2}{4} \cdot \frac{n^2}{\ln(n^2)} = \frac{\ln 2 \cdot n}{8 \cdot \ln n} \cdot n \geq n,$$

dabei gilt die letzte Abschätzung, sofern $\ln 2 \cdot n \geq 8 \cdot \ln n$ gilt, sofern also $\frac{\ln 2}{8} n \geq \ln n$ gilt. Es bleibt zu zeigen, dass diese Ungleichung für $n \geq 64$ richtig ist.

Beweis: Die Funktion

$$f(x) = \frac{\ln 2}{8} x - \ln x$$

ist nach ANA-2 (siehe den Anhang) für $x \geq \frac{8}{\ln 2} \approx 11,84$ monoton wachsend. Für $x = 64 = 2^6$ ist

$$f(64) = \frac{\ln 2}{8} 64 - 6 \ln 2 = \ln 2 (8 - 6) \ln 2 = 2 \ln 2 \approx 1,386,$$

also $f(64) > 1$, und demnach $f(n) > 1$ für $n \geq 64$.

**Umformulierung.** *Ist $p_n$ die $n$-te Primzahl und $n \geq 2$, so ist $p_n \leq n^2$.*

Dabei bezeichnen wir mit $p_k$ die $k$-te Primzahl, also $p_1 = 2,\ p_2 = 3,\ p_3 = 5$, usw.

Beweis: Die Ungleichung $\pi(n^2) \geq n$ besagt, dass es mindestens $n$ Primzahlen $p$ mit $p \leq n^2$ gibt. Die $n$-te Primzahl $p_n$ muss demnach im Intervall $[1, n^2]$ liegen, es muss also $p_n \leq n^2$ gelten.

### 1.7. Das Wachstum der Primzahlen.

**Satz.** *Es gibt positive reelle Zahlen $A < 1 < B$, mit*

$$\boxed{A \cdot n \cdot \ln n \ \leq\ p_n \ \leq\ B \cdot n \cdot \ln n,}$$

*zum Beispiel $A = \frac{1}{6 \cdot \ln 2}$, und $B = \frac{8}{\ln 2}$.*

Beachte: Die erste Ungleichung liefert einen weiteren Beweis für den Satz von Euklid und zwar mit einer quantitativen Aussage. Dabei muss man allerdings die Aussage folgendermaßen lesen: Für jedes $n$ gibt es die $n$-te Primzahl $p_n$ und es gilt $A \cdot n \cdot \ln n \ \leq\ p_n$.

Beweis des Satzes: Wir wissen, dass es $b > 1$ gibt mit $\pi(x) \leq b \cdot \frac{x}{\ln x}$. Nun ist $\pi(p_n) = n$, also gilt:

$$n = \pi(p_n) \leq b\frac{p_n}{\ln p_n} = b\frac{p_n}{\ln p_n},$$

also

$$p_n \geq \frac{1}{b} \cdot n \cdot \ln p_n \geq \frac{1}{b} \cdot n \cdot \ln n$$

(denn $p_n \geq n$). Nimm also $A = \frac{1}{b}$.

Nun zur oberen Abschätzung. Verwende die Formel $a\frac{x}{\ln x} \leq \pi(x)$ für $x = p_n$, also $\pi(p_n) = n$:

$$a \cdot \frac{p_n}{\ln p_n} \leq \pi(p_n) = n,$$

also

$$p_n \leq \frac{1}{a} \cdot n \cdot \ln p_n \leq \frac{1}{a} \cdot n \cdot \ln(n^2) = \frac{2}{a} \cdot n \cdot \ln n$$

(dabei verwenden wir $p_n \leq n^2$). Nimm also $B = \frac{2}{a}$.

**Folgerung.** *Die Reihe $\sum_p \frac{\ln p}{p}$ ist divergent.*

Beweis: Wegen $p_n \geq n$ und $p_n \leq B \cdot n \cdot \ln n$ gilt

$$\sum_{n=1}^{m} \frac{\ln p_n}{p_n} \;\geq\; \sum_{n=1}^{m} \frac{\ln n}{B \cdot n \cdot \ln n} = \frac{1}{B} \sum_{n=1}^{m} \frac{1}{n}.$$

Die Reihe $\sum_p \frac{\ln p}{p}$ majorisiert also das $\frac{1}{B}$-Fache der harmonischen Reihe $\sum_n \frac{1}{n}$. Nun ist aber die harmonische Reihe divergent, daraus folgt die Behauptung.

**Hinweis.** Es gilt sogar: Die Reihe $\sum_p \frac{1}{p}$ ist divergent, siehe Abschnitt 1.1.

### 1.8. Abschätzungen für $\pi(2n) - \pi(n)$.

**Satz.** Es gibt positive reelle Zahlen $a' < 1 < b'$ mit

$$\boxed{a' \frac{x}{\ln x} \;\leq\; \pi(2x) - \pi(x) \;\leq\; b' \frac{x}{\ln x} \qquad \text{für} \qquad x \geq 1,}$$

zum Beispiel $a' = 0,03, \quad b' = 2 \cdot \ln 2$.

Beweis: Die obere Abschätzung (sie ist aber weniger interessant!) wurde schon im Beweis von Satz 1.5 notiert, nämlich als Abschätzung (a).

Wir wenden uns also der unteren Schranke zu. Wir argumentieren wie im Beweis des Bertrand'schen Postulats, nur arbeiten wir jetzt konstruktiv. Dort hatten wir die Annahme $d = 1$ zum Widerspruch geführt, hier nun schätzen wir $d$ ab.

Aus

$$\frac{4^n}{2n} < \binom{2n}{n} = a \cdot b \cdot d \;\leq\; (2n)^{\frac{1}{2}\sqrt{2n}-1} \cdot 4^{\frac{2}{3}n} \cdot d$$

folgt

$$\boxed{4^{\frac{n}{3}} \cdot (2n)^{-\frac{1}{2}\sqrt{2n}} < d.}$$

Nun gilt

$$d = \prod_{n<p\leq 2n} \binom{2n}{n}_p \leq \prod_{n<p\leq 2n} 2n = (2n)^{\pi(2n)-\pi(n)},$$

also

$$4^{\frac{n}{3}} \cdot (2n)^{-\frac{1}{2}\sqrt{2n}} \leq (2n)^{\pi(2n)-\pi(n)}.$$

Logarithmieren liefert

$$\frac{n}{3} \ln 4 - \frac{1}{2}\sqrt{2n} \ln(2n) \;<\; (\pi(2n) - \pi(n)) \ln(2n),$$

also

$$\pi(2n) - \pi(n) \;>\; \frac{n}{\ln(2n)} \cdot \frac{\ln 4}{3} \;-\; \frac{1}{2}\sqrt{2n}.$$

Um die rechte Seite zu vereinfachen, verwenden wir erstens, dass gilt:

$$\ln(2n) = \ln 2 + \ln n \leq 2 \ln n$$

für $2 \leq n$. Zweitens zeigen wir, dass

$$\frac{1}{2}\sqrt{2n} \;\leq\; \frac{1}{5}\frac{n}{\ln(n)}$$

für $n \geq 500$ gilt.

Die Funktion $g(x) = \frac{x}{\ln x}$ ist nach ANA-3 für $x \geq e \approx 2,718$ monoton wachsend. Es ist $g(120) = \frac{120}{\ln 120} \approx 25,065$. Also ist $g(x) \geq 25$ für $x \geq 120$. Wir betrachten nun die Funktion

$$f(x) = \frac{2}{25}x - (\ln x)^2.$$

Nach ANA-4 (mit $a = \frac{2}{25}$) ist diese Funktion monoton wachsend, falls $\frac{x}{\ln x} \geq \frac{2}{a} = 25$ ist. Insgesamt sehen wir: Ist $x \geq 120$, so ist $\frac{x}{\ln x} \geq 25$ und damit ist $f(x)$ monoton wachsend. Nun ist

$$f(500) = \frac{2}{25}500 - (\ln 500)^2 = 40 - (\ln 500)^2,$$

und $(\ln 500)^2 \approx 38,6$. Es ist also $f(500) > 0$, und wegen des monotonen Wachstums ist $f(x) > 0$ für $x \geq 500$. Sei also $n \geq 500$. Wegen $f(n) \geq 0$ gilt

$$(\ln n)^2 \leq \frac{2}{25}n,$$

also erhalten wir

$$\frac{1}{2}n \leq \frac{1}{25}\frac{n^2}{(\ln n)^2}.$$

Wurzelziehen liefert die gesuchte Ungleichung:

$$\frac{1}{2}\sqrt{2n} = \sqrt{n/2} \;\leq\; \frac{1}{5}\frac{n}{\ln n}.$$

Insgesamt sehen wir:

$$\begin{aligned}\frac{n}{\ln(2n)} \cdot \frac{\ln 4}{3} \;-\; \frac{1}{2}\sqrt{2n} \;&\geq\; \frac{n}{2\ln n} \cdot \frac{\ln 4}{3} \;-\; \frac{1}{5}\frac{n}{\ln(n)} \\ &= \Big(\frac{\ln 4}{6} - \frac{1}{5}\Big)\frac{n}{\ln(n)}\end{aligned}$$

Es ist $\frac{\ln 4}{6} - \frac{1}{5} > 0,03$, also sehen wir

$$\pi(2n) - \pi(n) \ > \ 0,03\frac{n}{\ln(n)} \qquad \text{für} \qquad n \geq 500.$$

Dass diese Abschätzung auch für $n < 500$ gilt, kann man mit Hilfe einer Primzahltafel verifizieren.

**Folgerung.** *Zu jeder natürlichen Zahl $n > 5$ gibt es mindestens zwei Primzahlen $p$ mit $n < p < 2n$.*

Beweis: Für große $n$ (nämlich $n \geq 500$) wurde gerade bewiesen, dass $\pi(2n)-\pi(n) \geq 0,03\frac{n}{\ln(n)}$ gilt. Nun ist aber $0,03 \cdot \frac{500}{\ln 500} > 2$. Da $\pi(2n) - \pi(n)$ eine ganze Zahl ist, folgt aus $\pi(2n) - \pi(n) > 2$, dass sogar $\pi(2n) - \pi(n) \geq 3$ gilt: wir sehen also: Ist $n \geq 500$, so gibt es mindestens 3 Primzahlen $p$ mit $n < p \leq 2n$. Für kleine $n$ braucht man eine genügend lange Folge von Primzahlen $7 = q_1 < q_2 < \ldots$ mit $q_k < 2q_{k-2}$, etwa die Folge

$$7, 11, 13, 19, 23, 37, 43, 73, 83, 139, 163, 277, 317, 547, 631.$$

Beachte: Die Voraussetzung $n > 5$ wird wirklich gebraucht, denn für $n = 5$ gibt es nur die Primzahl $p = 7$ mit $5 < p < 10$.

**Nachtrag: ANA - Einige analytische Abschätzungen reeller Funktionen.**

Wir notieren hier einige Ungleichungen für reelle Funktion:

(1) $x + 1 \leq 2^x$ für $x \geq 1$.

Beweis: Für $x = 1$ gibt die Behauptung. Es reicht zu zeigen, dass die Differenzfunktion $f(x) = 2^x - x - 1$ monoton wächst. Die Ableitung ist $f'(x) = \ln 2 \cdot 2^x - 1 > 0$, denn für $x \geq 1$ ist $2^x \geq 2 > \frac{1}{\ln 2}$ (es ist $\ln 2 \approx 0,69$ und demnach $\frac{1}{\ln 2} \approx 1,44$).

(2) Sei $a > 0$. Die Funktion

$$f(x) = ax - \ln x$$

für $x > 0$ hat bei $x = \frac{1}{a}$ ein Minimum; im Intervall $[\frac{1}{a}, \infty)$ ist sie monoton wachsend (und unbeschränkt).

Es ist $f'(x) = a - \frac{1}{x}$, also gilt $f'(x) = 0$ nur für $x = \frac{1}{a}$. Und natürlich ist $a - \frac{1}{x}$ für $x > 0$ streng monoton wachsend, also ist $f'(x)$ im Intervall $(0, \frac{1}{a})$ negativ und im Intervall $(\frac{1}{a}, \infty)$ positiv.

(3) Sei $c > 0$. Die Funktion $c\frac{x}{\ln x}$ hat bei $e$ ein Minimum, im Intervall $[e, \infty)$ ist sie streng monoton wachsend (und unbeschränkt).

Sei also $f(x) = c\frac{x}{\ln x}$. Es ist $f'(x) = c\big(\frac{1}{\ln x} - \frac{1}{(\ln x)^2}\big)$. Ist $x > e$, so ist $\ln x > 1$, also $\frac{1}{\ln x} - \frac{1}{(\ln x)^2} > 0$, und demnach ist $f(x)$ streng monoton wachsend.

(4) Sei $a > 0$. Die Funktion $f(x) = ax - (\ln x)^2$ ist für $\frac{x}{\ln x} \geq \frac{2}{a}$ streng monoton wachsend (und unbeschränkt).

Es ist $f'(x) = a - \frac{2\ln x}{x}$. Ist $\frac{x}{\ln x} > \frac{2}{a}$, so ist $a > \frac{2\ln x}{x}$, also $f'(x) > 0$.