

Universität Paderborn  
Fakultät 5: Elektrotechnik, Informatik, Mathematik

Proseminararbeit  
Thema: Das Postulat von Bertrand

Proseminar: Analysis  
Betreuer: Prof. Dr. Joachim Hilgert  
Studienjahr: Sommersemester 2005  
Matrikelnummer: 6272805  
Name, Vorname: Winzenick, Jennyfer  
Anschrift: Hunikastr. 14, 33129 Delbrück  
Abgabedatum: 15. April 2005

# Inhaltsverzeichnis

1	Primzahlen	1
2	Der Binominalkoeffizient	7
3	Bertrands Postulat	10

## 1 Primzahlen

Dieser Abschnitt wurde zum Teil aus dem Buch [5] übernommen. Eine etwas abstraktere Darstellung, allerdings mit denselben Ergebnissen findet sich beispielsweise in [2].

**Definition 1.1.** Ein Element  $d \in \mathbb{N}$  heißt ein Teiler des Elements  $a \in \mathbb{N}$ , in Zeichen  $d \mid a$ , wenn es ein Element  $k \in \mathbb{N}$  gibt, so dass gilt:  $a = k \cdot d$ . Man sagt dann auch  $d$  teilt  $a$  oder  $a$  ist ein Vielfaches von  $d$ . Ist  $d$  kein Teiler von  $a$ , so schreibt man  $d \nmid a$ .

**Proposition 1.2.** Es seien  $a, b, c, d \in \mathbb{N}$ . Dann gilt:

1.  $a \mid a$  (Reflexivität).
2. Aus  $a \mid b$  und  $b \mid c$  folgt  $a \mid c$  (Transitivität).
3. Aus  $a \mid b$  und  $c \mid d$  folgt  $ac \mid bd$ .
4. Aus  $a \mid b$  und  $a \mid c$  folgt  $a \mid (xb + yc)$  für alle  $x, y \in \mathbb{N}$ .

*Beweis.* 1. Es ist  $1 \in \mathbb{N}$ . Wegen  $a = 1 \cdot a$  folgt also  $a \mid a$ .

2. Es gelten  $a \mid b$  und  $b \mid c$ . Dann gibt es  $k, l \in \mathbb{N}$  mit  $ka = b$  und  $lb = c$ . Setzt man die erste Gleichung für  $b$  in die zweite Gleichung ein, erhält man

$$c = lb = l(ka) = (lk)a$$

mit  $lk \in \mathbb{N}$ . Also folgt  $a \mid c$ .

3. Es gelten  $a \mid b$  und  $c \mid d$ . Dann gibt es  $k, l \in \mathbb{N}$  mit  $ka = b$  und  $lc = d$ .  
Multipliziert man beide Gleichungen miteinander, so erhält man

$$bd = (ka) \cdot (lc) = (kl) \cdot (ac).$$

Wegen  $kl \in \mathbb{N}$  folgt also  $ac \mid bd$ .

4. Aus  $b = ka$  und  $c = la$  für  $k, l \in \mathbb{N}$  folgt

$$xb + yc = x(ka) + y(la) = (xk + yl)a$$

mit  $xk + yl \in \mathbb{N}$ . Also folgt  $a \mid xb + yc$ .

□

**Proposition 1.3.** *Es sei  $a \in \mathbb{N}$  und  $d \in \mathbb{N}$  ein Teiler von  $a$ . Dann gilt  $d \leq a$ . Insbesondere hat eine natürliche Zahl  $a$  höchstens endlich viele verschiedene Teiler.*

*Beweis.* Die Behauptung folgt unmittelbar aus der Definition: Gilt  $d \mid a$ , so gibt es ein  $k \in \mathbb{N}$ , so dass  $a = k \cdot d$  ist. Wegen  $k \geq 1$  folgt also  $a \geq d$ . Es gibt nur maximal  $a$  unterschiedliche natürliche Zahlen, die kleiner oder gleich  $a$  sind, also kann es auch nur maximal  $a$  unterschiedliche Teiler einer Zahl  $a \in \mathbb{N}$  geben. □

**Definition 1.4.** 1. *Es sei  $a \in \mathbb{N}$ . Dann heißen  $a$  und  $1$  die trivialen Teiler von  $a$ . Ein Teiler von  $a$ , der nicht trivial ist, heißt echter Teiler.*

2. *Eine natürliche Zahl  $p > 1$  heißt Primzahl, wenn  $p$  nur dann als Produkt  $ab$  der Zahlen  $a, b \in \mathbb{N}$  geschrieben werden kann, wenn  $a = 1$  oder  $b = 1$  folgt. Die Menge aller Primzahlen wird mit  $\mathbb{P}$  bezeichnet.*

**Proposition 1.5.** *Jede Zahl natürliche Zahl  $a > 1$  besitzt einen kleinsten Teiler  $t > 1$ .*

*Dieser Teiler ist eine Primzahl.*

*Beweis.* Es sei  $a \in \mathbb{N}$ ,  $a > 1$  beliebig. Betrachte die Menge

$$T := \{t \in \mathbb{N} : t \neq 1 \text{ und } t \mid a\}.$$

Wegen  $a \mid a$  ist  $T \neq \emptyset$ . Nach dem Minimalprinzip<sup>1</sup> für natürliche Zahlen hat  $T$  ein kleinstes Element. Zu zeigen bleibt, dass diese Zahl  $t_{\min}$  eine Primzahl ist:

Angenommen  $t_{\min}$  wäre keine Primzahl. Dann gäbe es eine Zahl  $1 < k < t_{\min}$  mit  $k \mid t_{\min}$ . Aus 1.2 auf Seite 1 folgt dann aber dass  $k$  ein Teiler von  $a$  wäre und somit in  $T$  enthalten wäre. Dies ist ein Widerspruch zu der Minimalität von  $t_{\min}$ . Also ist das kleinste Element von  $T$  eine Primzahl.  $\square$

**Satz 1.6.** (Euklid) *Es gibt unendlich viele Primzahlen.*

*Beweis.* Angenommen, es gäbe nur endlich viele Primzahlen, d.h.  $\mathbb{P} := \{p_1, \dots, p_n\}$  für ein  $n \in \mathbb{N}$ . Betrachte

$$q := \prod_{k=1}^n p_k + 1.$$

Es kann  $q$  keine Primzahl sein, da für alle Primzahlen  $p_k \in \mathbb{P}$  gilt  $q > p_k$ . Es sei  $t > 1$  der kleinste Teiler von  $q$ . Nach 1.5 auf der vorherigen Seite gilt also  $t \in \mathbb{P}$ . Somit gilt  $t \mid q$  und  $t \mid q - 1$ , also teilt  $t$  nach 1.2 auf Seite 1 auch  $q + (-1)(q - 1) = 1$ . Dies ist ein Widerspruch zu  $t > 1$ .  $\square$

**Definition 1.7.** *Es sei  $a \in \mathbb{N}$ ,  $a > 1$ . Dann heißt jede Primzahl  $p$ , die  $a$  teilt, ein Primteiler oder Primfaktor von  $a$ . Eine Darstellung*

$$a = p_1 \cdot \dots \cdot p_n$$

*mit (nicht zwingend paarweise verschiedenen) Primfaktoren  $p_1, \dots, p_n$  heißt Primfaktorzerlegung von  $a$ .*

---

<sup>1</sup>Vergleiche [3], Anhang A, Axiom A.1.2

**Satz 1.8.** (*Hauptsatz der Zahlentheorie*) Jede natürliche Zahl  $a$  besitzt eine bis auf Reihenfolge eindeutige Primfaktorzerlegung.

*Beweis.* Der Beweis des Hauptsatzes der Zahlentheorie wird als Induktion geführt. Dabei wird im Induktionsschritt die Existenz und die Eindeutigkeit getrennt gezeigt.

**Induktionsanfang:** Es sei  $a = 1$ . Vereinbarungsgemäß ist das Produkt ohne Faktor gleich Eins, d.h. es gibt eine Primfaktorzerlegung der Zahl 1. Diese ist eindeutig, da  $p > 1$  für alle  $p \in \mathbb{P}$  gilt und somit ein Produkt mit beliebig vielen Primfaktoren genau dann 1 ist, wenn die Zahl der Faktoren gerade Null ist.

**Induktionsvoraussetzung:** Es sei  $a > 1$  eine beliebige natürliche Zahl. Dann besitzt jede natürliche Zahl  $n < a$  eine eindeutige Primfaktorzerlegung.

**Induktionsschluss für die Existenz:** Ist  $a$  eine Primzahl, so ist  $a$  bereits ein Produkt von Primzahlen. Betrachte den Fall, dass  $a$  keine Primzahl ist. Dann besitzt  $a$  einen minimalen Primteiler  $t$  mit  $1 < t < a$ . Damit ist  $c := \frac{a}{t}$  eine natürliche Zahl mit  $c < a$ , d.h.  $c$  besitzt eine Primfaktorzerlegung  $c = p_1 \cdot \dots \cdot p_k$ . Dann ist  $a = t \cdot p_1 \cdot \dots \cdot p_k$  eine Primfaktorzerlegung von  $a$ .

**Induktionsschluss für die Eindeutigkeit:** Es seien

$$a = p_1 \cdot \dots \cdot p_k \text{ und } a = q_1 \cdot \dots \cdot q_l$$

Primfaktorzerlegungen von  $a$ . Die Primfaktoren seien o.B.d.A der Größe nach sortiert<sup>2</sup> und es gelte o.B.d.A  $p_1 \leq q_1$ . Es sei

$$b := p_2 \cdot \dots \cdot p_k.$$

---

<sup>2</sup>Es gelte also  $p_1 \geq p_2 \geq \dots \geq p_k$  und  $q_1 \geq q_2 \geq \dots \geq q_l$ .

1. Fall: Es gibt einen Index  $j \in \{1, \dots, l\}$ , so dass  $p_1 = q_j$  ist. Dann gilt

$$b = p_2 \cdot \dots \cdot p_k = q_1 \cdot \dots \cdot q_{j-1} \cdot q_{j+1} \cdot \dots \cdot q_l.$$

Nach Induktionsvoraussetzung ist wegen  $b < a$  die Primfaktorzerlegung von  $b$  bis auf Reihenfolge eindeutig, d.h. nach der oben angegebenen Nummerierung ist  $p_1 = q_1$  und für die Primfaktorzerlegung von  $b$  gilt  $p_i = q_i$  für  $i = 2, \dots, k$ . Demnach ist auch die Primfaktorzerlegung von  $a = p_1 \cdot b$  eindeutig.

2. Fall: Für alle  $j = 1, \dots, l$  gelte  $p_1 \neq q_j$ . Setze

$$c := q_2 \cdot \dots \cdot q_l.$$

Dann gilt:

$$a = p_1 b = q_1 c \text{ mit } p_1 < q_1.$$

Damit ist  $a' = a - p_1 c \in \mathbb{N}$  und es gilt

$$a' = p_1(b - c) = (q_1 - p_1)c,$$

wobei alle gegebenen Faktoren sowie  $a'$  größer oder gleich 1 und kleiner als  $a$  sind. Nach Induktionsvoraussetzung besitzen also alle Faktoren und  $a'$  eine eindeutige Primfaktorzerlegung. Insbesondere folgt daher<sup>3</sup>:

$$p_1 \mid a \Rightarrow p_1 \mid (q_1 - p_1) \text{ oder } p_1 \mid c,$$

da  $p_1$  ein Primfaktor von  $a'$  ist.  $p_1$  ist nach Voraussetzung kein Primfaktor von  $c$ , es folgt also  $p_1 \mid (q_1 - p_1)$  und damit  $p_1 \mid q_1$ . Dies ist wegen  $1 < p_1 < q_1$  ein Widerspruch dazu, dass  $q_1$  eine Primzahl ist.

□

---

<sup>3</sup>Dieses Ergebnis wird in der Proposition 1.9 gefasst.

**Proposition 1.9.** *Es sei  $p \in \mathbb{N}$  eine natürliche Zahl. Dann sind folgende Aussagen äquivalent:*

1.  $p$  ist eine Primzahl.
2. Aus  $p \mid (ab)$  für  $a, b \in \mathbb{N}$  folgt  $p \mid a$  oder  $p \mid b$ .

*Beweis.* Zeige die Äquivalenz durch zwei Implikationen:

“1.  $\Rightarrow$  2.” Es sei  $p$  eine Primzahl. Aus  $p \mid (ab)$  folgt, dass  $p$  in der Primfaktorzerlegung von  $ab$  vorkommt. Wegen der Eindeutigkeit muss  $p$  also ein Primfaktor von  $a$  oder von  $b$  sein.

“2.  $\Rightarrow$  1.” Es sei  $d$  ein beliebiger Teiler von  $p$ . Dann gibt es ein  $k \in \mathbb{N}$  mit  $p = dk$ . Insbesondere gilt  $p \mid dk$ . Nach Voraussetzung gilt dann  $p \mid d$  oder  $p \mid k$ , d.h.  $p = d$  oder  $p = k$ . Aus zweitem folgt  $d = 1$ . Also sind die einzigen Teiler von  $p$  die trivialen Teiler, d.h.  $p$  ist eine Primzahl.

□

**Proposition 1.10.** *Es sei  $N \in \mathbb{N}$  beliebig. Dann gibt es ein  $n \in \mathbb{N}$ , so dass zwischen  $n$  und  $n + N$  keine Primzahl liegt, d.h. der Abstand zweier aufeinanderfolgender Primzahlen kann beliebig groß werden.*

*Beweis.* Es sei  $p > N$  eine Primzahl,  $n := \prod_{q \leq p} q$  das Produkt aufeinanderfolgender Primzahlen. Dann sind die Zahlen  $n + k$  für  $1 < k < p$  keine Primzahlen, denn  $k$  besitzt einen Primfaktor  $q < p$ , d.h. es folgt mit  $q \mid k$  und  $q \mid n$ , dass  $q$  ein Teiler von  $n + k$  ist. □

**Ausblick 1.11.** *Bisher wurde gezeigt, dass es unendlich viele Primzahlen gibt, und dass die Differenz zweier aufeinanderfolgender Primzahlen unendlich groß sein kann. Andererseits lässt sich aber auch eine Abschätzung dafür geben, wo ausgehend von einer beliebigen Zahl spätestens die nächste Primzahl zu finden ist. Eine solche Abschätzung gibt das Postulat von Bertrand:*

*Ist  $n \in \mathbb{N}$  eine beliebige natürliche Zahl, so gibt es eine Primzahl  $p \in \mathbb{P}$ , mit  $n < p \leq 2n$ .*

Ein Beweis dieses Satzes wird in Abschnitt 3 gegeben.

## 2 Der Binominalkoeffizient

In diesem Abschnitt wird der Binominalkoeffizient eingeführt und einige Rechenregeln für diesen bewiesen. Die Ausführungen stammen im Wesentlichen aus [1].

**Definition 2.1.** 1. Für eine natürliche Zahl  $n \in \mathbb{N}$  definieren wir die Fakultät  $n!$  durch

$$n! := 1 \cdot 2 \cdot \dots \cdot n.$$

2. Für natürliche Zahlen  $n, k \in \mathbb{N}$  setzt man

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

Die Zahlen  $\binom{n}{k}$  heißen Binominalkoeffizienten und man sagt dazu “ $n$  über  $k$ ”.

**Proposition 2.2.** Für  $n, k \in \mathbb{N}$  gelten:

1.  $\binom{n}{k} = 0$  für  $k > n$ .
2.  $\binom{n}{k} = \binom{n}{n-k}$  für  $n \geq k$ .

*Beweis.* 1. Ist  $k > n$ , so ist einer der Faktoren des Zählers und somit der gesamte Bruch gleich Null.

2. Diese Gleichheit folgt unmittelbar aus der Definition.

□

**Proposition 2.3.** Für  $n \geq k$  gilt:  $\binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1}$ .

*Beweis.* Für  $k \leq n$  folgt:

$$\begin{aligned}\binom{n}{k} + \binom{n}{k+1} &= \frac{n!}{k!(n-k)!} + \frac{n!}{(k+1)! \cdot (n-k-1)!} \\ &= \frac{n!}{k!(n-k)!} + \frac{n!}{k!(n-k)!} \cdot \frac{n-k}{k+1} \\ &= \frac{n!}{k!(n-k)!} \cdot \left(1 + \frac{n-k}{k+1}\right) \\ &= \frac{n!}{k!((n+1)-(k+1))!} \cdot \frac{n+1}{k+1} \\ &= \frac{(n+1)!}{(k+1)!((n+1)-(k+1))!} = \binom{n+1}{k+1}\end{aligned}$$

□

**Satz 2.4.** (*Binomischer Lehrsatz*) Es seien  $x, y \in \mathbb{R}$  und  $n \in \mathbb{N}$ . Dann gilt:

$$(x+y)^n = \sum_{k=0}^n \binom{n}{k} x^{n-k} y^k.$$

*Beweis.* Der Beweis des Binomischen Lehrsatzes erfolgt durch vollständige Induktion nach  $n$ :

**Induktionsanfang** Sei  $n = 1$ , dann gilt:

$$(x+y)^1 = x+y = \binom{1}{0}x + \binom{1}{1}y.$$

## Induktionsschluss

$$\begin{aligned}
 (x+y)^{n+1} &= (x+y) \cdot (x+y)^n = (x+y) \cdot \sum_{k=0}^n \binom{n}{k} x^{n-k} y^k \\
 &= x \cdot \sum_{k=0}^n \binom{n}{k} x^{n-k} y^k + y \sum_{k=0}^n \binom{n}{k} x^{n-k} y^k \\
 &= \sum_{k=0}^n \binom{n}{k} x^{n-k+1} y^k + \sum_{k=0}^n \binom{n}{k} x^{n-k} y^{k+1} \\
 &= x^{n+1} + \sum_{k=1}^n \binom{n}{k} x^{n-k+1} y^k + \sum_{k=0}^{n-1} \binom{n}{k} x^{n-k} y^{k+1} + y^{n+1} \\
 &= x^{n+1} + \sum_{k=1}^n \binom{n}{k} x^{n-k+1} y^k + \sum_{k=1}^n \binom{n}{k-1} x^{n-k+1} y^k + y^{n+1} \\
 &= x^{n+1} + \sum_{k=1}^n \left( \binom{n}{k} + \binom{n}{k-1} \right) x^{n-k+1} y^k + y^{n+1} \\
 &= \binom{n+1}{0} x^{n+1} + \sum_{k=1}^n \binom{n+1}{k} x^{n-k+1} y^k + \binom{n+1}{n+1} y^{n+1} \\
 &= \sum_{k=0}^{n+1} \binom{n+1}{k} x^{n-k+1} y^k.
 \end{aligned}$$

□

**Folgerung 2.5.** 1.  $\sum_{k=0}^n \binom{n}{k} = 2^n$

2.  $\binom{n}{k}$  ist für  $n, k \in \mathbb{N}$  eine natürliche Zahl.

*Beweis.* 1. Folgt für  $x = 1$  und  $y = 1$  unmittelbar aus dem Binomischen Lehrsatz.

2. Der Binominalkoeffizient im Binomischen Lehrsatz gibt gerade an, wie oft das Produkt  $x^{n-k} y^k$  beim Ausrechnen des Binoms vorkommt. Diese Anzahl ist eine natürliche Zahl.

□

### 3 Bertrands Postulat

In diesem letzten Abschnitt, soll das in Abschnitt 1 bereits angegebene Postulat von Bertrand bewiesen werden. Dazu werden zu Beginn des Abschnitts noch einige Rechenregeln bewiesen, die unter anderem den Zusammenhang zwischen Primzahlen und Binominalkoeffizienten verdeutlichen. Der Beweis des Postulats von Bertrand stammt dabei aus [4].

**Hilfssatz 3.1.** *Für eine natürliche Zahl  $m \geq 1$  und Primzahlen  $p \in \mathbb{P}$  gilt die Abschätzung*

$$\prod_{m+1 < p \leq 2m+1} p \leq \binom{2m+1}{m}$$

*Beweis.* Es ist  $\binom{2m+1}{m}$  eine natürliche Zahl, d.h. sie besitzt eine bis auf Reihenfolge eindeutige Primfaktorzerlegung. Da Primzahlen keine echten Teiler besitzen und die größten Faktoren des Nenners  $m+1$  sind, werden die Primzahlen des Zählers, die größer als  $m+1$  sind nicht durch Faktoren des Nenners gekürzt. Also ist jede Primzahl  $p$  mit  $m+1 < p \leq 2m+1$  in der Primfaktorzerlegung enthalten, d.h. es gilt die Behauptung.  $\square$

**Hilfssatz 3.2.** *Für natürliche Zahlen  $m \geq 1$  gilt:*

$$\binom{2m+1}{m} \leq 4^m.$$

*Beweis.* Es sei  $m \geq 1$  eine beliebige natürliche Zahl. Dann gilt:

$$\binom{2m+1}{m} = \binom{2m}{m} + \binom{2m}{m-1} \leq \sum_{k=1}^{2m} \binom{2m}{k} = 2^{2m} = 4^m.$$

$\square$

**Proposition 3.3.** *Für jedes  $x \in \mathbb{R}$  mit  $x \geq 2$  gilt die Abschätzung*

$$\prod_{p \leq x} p \leq 4^{x-1}.$$

*Beweis.* Es sei  $q$  die größte Primzahl, für die  $q \leq x$  gilt. Offensichtlich gilt

$$\prod_{p \leq q} p = \prod_{p \leq x} p,$$

sowie  $4^{q-1} \leq 4^{x-1}$ . Zu zeigen bleibt also, dass für jede Primzahl  $q \in \mathbb{P}$  gilt:

$$\prod_{p \leq q} p \leq 4^{q-1}.$$

Zeige dazu induktiv, dass folgende Behauptung für alle natürlichen Zahlen erfüllt ist:

**Behauptung:** Für alle  $n \in \mathbb{N}$  mit  $n \geq 2$  gilt:

$$\prod_{p \leq n} p \leq 4^{n-1}$$

**Induktionsanfang:** Betrachte  $n = 2$ : Die einzige Primzahl, die kleiner oder gleich 2 ist, ist die 2 selbst. Damit folgt:

$$\prod_{p \leq 2} p = 2 = 2^{2-1}$$

**Induktionsschluss:** Es sei nun  $n > 2$ . Dann gilt:

$$\prod_{p \leq n+1} p = \begin{cases} \prod_{p \leq n} p & \text{falls } n+1 \text{ keine Primzahl ist} \\ \prod_{p \leq n} p \cdot (n+1) & \text{falls } n+1 \text{ eine Primzahl ist} \end{cases}$$

Ist  $n+1$  keine Primzahl, dann folgt

$$\prod_{p \leq n+1} p = \prod_{p \leq n} p \leq 4^{n-1} \leq 4^n.$$

Betrachte also den Fall, dass  $n + 1$  prim ist. In diesem Fall ist  $n$  und  $n + 2$  gerade. Zerlege nun das Produkt in

$$\prod_{p \leq n+1} p = \prod_{p \leq \frac{n+2}{2}} p \cdot \prod_{\frac{n+2}{2} < p \leq n+1} p$$

Das erste Teilprodukt ist nach Induktionsanfang kleiner oder gleich  $4^{n/2}$ , das zweite Teilprodukt kann mit Hilfe von 3.1 und 3.2 abgeschätzt werden:

$$\prod_{\frac{n+2}{2} < p \leq n+1} p \leq \binom{n+1}{\frac{n}{2}} \leq 4^{n/2}.$$

Insgesamt folgt also:

$$\prod_{p \leq n+1} p \leq 4^{n/2} \cdot 4^{n/2} = 4^n.$$

□

**Proposition 3.4.** *Für alle  $n \in \mathbb{N}$  gilt die Abschätzung*

$$\binom{2n}{n} \geq \frac{4^n}{2n}$$

*Beweis.* Beweise diese Abschätzung durch vollständige Induktion nach  $n \in \mathbb{N}$ :

**Induktionsanfang** Es sei  $n = 1$ . Dann gilt:

$$\binom{2}{1} = \frac{2!}{1! \cdot 1!} = 2 = \frac{4^1}{2 \cdot 1}.$$

**Induktionsschluss** Die Behauptung gelte für ein beliebiges  $n \geq 1$ . Dann folgt:

$$\begin{aligned}
 \binom{2(n+1)}{n+1} &= \binom{2n+1}{n} + \binom{2n+1}{n+1} \\
 &= \left( \binom{2n}{n} + \binom{2n}{n-1} \right) + \left( \binom{2n}{n+1} + \binom{2n}{n} \right) \\
 &= 2 \cdot \binom{2n}{n} + 2 \cdot \binom{2n}{n+1} \\
 &= 2 \cdot \binom{2n}{n} + 2 \cdot \binom{2n}{n} \cdot \frac{n}{n+1} \\
 &= \binom{2n}{n} \cdot \left( 2 + \frac{2n}{n+1} \right) \\
 &\geq \frac{4^n}{2n} \cdot \frac{4n+2}{n+1} \\
 &= \frac{4n \cdot 4}{2(n+1)} \cdot \frac{n + \frac{1}{2}}{n} \\
 &= \frac{4^{n+1}}{2(n+1)}.
 \end{aligned}$$

□

**Hilfssatz 3.5.** *Es sei  $n \in \mathbb{N}$  beliebig. Die Primfaktorzerlegung von  $n!$  enthält dabei den Primfaktor  $p$  genau*

$$\sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor$$

*mal. Dieses Theorem geht auf Legendre zurück.*

*Beweis.* Es seien  $n, a \in \mathbb{N}$  beliebig. Dann werden genau die natürlichen Zahlen  $c \leq n$  durch  $a$  geteilt, für die es ein  $l \in \mathbb{N}$  gibt mit  $a \cdot l = c$ . Wegen der Beschränkung  $c \leq n$  folgt  $l \leq \lfloor \frac{n}{a} \rfloor$ . Es besitzen also genau die Zahlen  $l, 2l, \dots, \lfloor \frac{n}{l} \rfloor$  die Zahl  $l$  als Teiler.

Die Faktoren von  $n!$  sind gerade die natürlichen Zahlen kleiner oder gleich  $n$ . Davon gibt es jeweils  $\lfloor \frac{n}{p^k} \rfloor$ , die von  $p^k$  geteilt werden. Also besitzt  $n!$

den Primfaktor  $p$  genau  $\sum_{k=1}^{\infty} \lfloor \frac{n}{p^k} \rfloor$  mal. Der Laufindex  $k$  zählt dabei die Vielfachheit des Primfaktors  $p$  einer Zahl  $c \leq n$ .  $\square$

**Proposition 3.6.** *Es sei  $n \in \mathbb{N}$  beliebig und  $B = \prod_{k=1}^N p_k^{\mu_k}$  die Primfaktorzerlegung von  $B := \binom{2n}{n}$ . Dann gelten:*

1. Für alle  $k \leq n$  ist  $p_k^{\mu_k} \leq 2n$ .
2. Für alle  $p_k > \sqrt{2n}$  ist  $\mu_k \leq 1$ .
3. Für alle  $\frac{2}{3}n < p_k \leq n$  ist  $\mu_k = 0$ , d.h. es gibt keinen Primfaktor zwischen  $\frac{2}{3}n$  und  $n$ .

*Beweis.* 1. Nach 3.5 auf der vorherigen Seite besitzt die Zahl  $\binom{2n}{n} = \frac{(2n)!}{n!n!}$  den Primfaktor  $p$  genau

$$\sum_{k=1}^{\infty} \left\lfloor \frac{2n}{p^k} \right\rfloor - 2 \cdot \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor = \sum_{k=1}^{\infty} \left( \left\lfloor \frac{2n}{p^k} \right\rfloor - 2 \left\lfloor \frac{n}{p^k} \right\rfloor \right)$$

mal, wobei für jeden Summanden gilt:

$$\left\lfloor \frac{2n}{p^k} \right\rfloor - 2 \left\lfloor \frac{n}{p^k} \right\rfloor < \frac{2n}{p^k} - 2 \left( \frac{n}{p^k} - 1 \right) = 2.$$

mal. Also ist jeder Summand maximal Eins. Außerdem sind die Summanden für  $p^k > 2n$  gleich Null. Es folgt also für alle Exponenten der Primfaktoren:

$$\begin{aligned} \mu_k &= \sum_{k=1}^{\infty} \left( \left\lfloor \frac{2n}{p^k} \right\rfloor - 2 \left\lfloor \frac{n}{p^k} \right\rfloor \right) \\ &\leq \max\{r : p^r \leq 2n\}, \end{aligned}$$

d.h. es gilt  $p_k^{\mu_k} \leq 2n$  für alle  $k \leq n$ .

2. Eine unmittelbare Folgerung aus 1 ist, dass die Exponenten für  $p > \sqrt{2n}$  höchstens Eins sein können.

3. Für  $\frac{2}{3}n < p$  folgt  $2n < 3p$ , wobei  $p \leq \frac{n}{2}$  und  $2p > \frac{n}{2}$  ist. Es sind also  $p$  und  $2p$  Faktoren des Zählers und  $p$  zweimal Faktor des Nenners. Also gilt  $3p \nmid \binom{2n}{n}$ .

□

**Satz 3.7.** (Bertrands Postulat) Ist  $n \in \mathbb{N}$  eine beliebige natürliche Zahl, so gibt es eine Primzahl  $p \in \mathbb{P}$ , mit der Eigenschaft  $n < p \leq 2n$ .

**Beispiel 3.8.** Betrachte die Primzahlen

$$\begin{aligned} \mathbb{P}' &:= \{2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631, 1259, 2503, 4001\} \\ &= \{q_1, \dots, q_{14}\}. \end{aligned}$$

Die Aussage folgt aus  $2q_m \geq q_{m+1}$ : Es sei  $n \in \mathbb{N}$  mit  $q_m \leq n < q_{m+1}$  für ein  $m \in \mathbb{N}$  mit  $m \leq 14$ . Dann gilt:

$$2q_m \leq 2n < 2q_{m+1} \quad \Rightarrow \quad n < q_{m+1} \leq 2n.$$

*Beweis.* Nach 3.4 auf Seite 12 und 3.6 auf der vorherigen Seite gilt die Ungleichungskette

$$\frac{4^n}{2n} \leq \binom{2n}{n} \leq \prod_{p \leq \sqrt{2n}} 2n \cdot \prod_{\sqrt{2n} < p \leq \frac{2}{3}n} p \cdot \prod_{n < p \leq 2n} p.$$

Da es nur maximal  $\sqrt{2n} + 1$  Primzahlen gibt, die kleiner oder gleich  $\sqrt{2n}$  sind, kann das erste Teilprodukt sehr leicht abgeschätzt werden. Durch 3.3 auf Seite 10 kann auch das zweite Produkt abgeschätzt werden und es folgt:

$$4^n \leq (2n)^{1+\sqrt{2n}} \cdot 4^{\frac{2}{3}n} \cdot \prod_{n < p \leq 2n} p.$$

Angenommen, es gäbe keine Primzahl zwischen  $n$  und  $2n$ . Dann wäre das letzte Produkt Eins und durch Umstellen der Ungleichung erhält man:

$$4^n \leq (2n)^{3(1+\sqrt{2n})} \tag{1}$$

Induktiv lässt sich zeigen, dass für alle  $a \in \mathbb{N}$  gilt:  $a + 1 \leq 2^a$ . Daraus ergibt sich die Ungleichungskette

$$2n = (\sqrt[6]{2n})^6 < (\lfloor \sqrt[6]{2n} \rfloor + 1)^6 < \left(2^{\lfloor \sqrt[6]{2n} \rfloor}\right)^6 \leq 2^{6 \cdot \sqrt[6]{2n}}.$$

Setzt man dieses Ergebnis in (1) ein, so ergibt sich für  $n \geq 50$ :<sup>4</sup>

$$\begin{aligned} 2^{2n} &\leq (2n)^{3(1+\sqrt{2n})} < \left(2^{6 \sqrt[6]{2n}}\right)^{3+3\sqrt{2n}} \\ &< (2)^{\sqrt[6]{2n}(18+18\sqrt{2n})} < 2^{20 \sqrt[6]{2n}\sqrt{2n}} = 2^{20(2n)^{2/3}} \end{aligned}$$

Stellt man die Ungleichung  $2^n < 2^{20(2n)^{2/3}}$  nach  $n$  um, so erhält man:

$$\begin{aligned} 2n < 20(2n)^{2/3} &\Rightarrow (2n)^{1/3} < 20 \\ &\Rightarrow n < 4000. \end{aligned}$$

Damit lässt sich feststellen, dass es nur möglich ist, für eine natürliche Zahl  $50 < n < 4000$  keine Primzahl  $p$  zu finden, so dass  $n < p \leq 2p$  gilt. Diese Zahlen wurden jedoch bereits im Beispiel 3.8 auf der vorherigen Seite behandelt. Also gilt Bertrands Postulat für alle natürlichen Zahlen  $n \in \mathbb{N}$ .  $\square$

---

<sup>4</sup>In der Ungleichungskette wird genutzt, dass  $18 < 2\sqrt{2n}$  ist. Dies ist genau dann der Fall, wenn  $9^2 < 2n$  ist, bzw. grob abgeschätzt  $n > 50$  gilt.

## Literatur

- [1] Otto Forster. *Analysis 1*. Vieweg, 1983.
- [2] Gerhard Frey. *Elementare Zahlentheorie*. Vieweg, 1984.
- [3] Joachim Hilgert. *Analysis I*. Vorlesungsskript, 2004.
- [4] Martin Aigner und Günter M. Ziegler. *Proofs from the Book*. Springer Verlag, 1998.
- [5] Reinhold Remmert und Peter Ullrich. *Elementare Zahlentheorie*. Birkhäuser, 1995.