

## 2. Verteilung der Primzahlen. Bertrands Postulat

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

*Beweis.* Wir zeigen, dass es zu jeder endlichen Menge  $p_1, p_2, \dots, p_n$  von Primzahlen immer noch eine weitere Primzahl  $q$  gibt, die von allen  $p_j$ , ( $1 \leq j \leq n$ ), verschieden ist. Dazu betrachten wir die Zahl

$$Q := p_1 p_2 \cdot \dots \cdot p_n + 1.$$

Dann ist  $Q$  entweder selbst eine Primzahl oder besitzt einen Primfaktor  $q \mid Q$ . Dieser ist von allen  $p_j$  verschieden, da  $p_j \nmid Q$  für alle  $j$ .

**2.2. Anzahl der Primzahlen.** Für eine reelle Zahl  $x \geq 0$  bezeichnen wir mit  $\pi(x)$  die Anzahl aller Primzahlen  $p \leq x$ . Z.B. ist  $\pi(1) = 0$ ,  $\pi(\sqrt{5}) = 1$ ,  $\pi(10) = 4$ . Einige größere Werte sind

$$\pi(100) = 25, \quad \pi(1000) = 168, \quad \pi(10^6) = 79498.$$

Nach Satz 2.1 gilt jedenfalls

$$\lim_{x \rightarrow \infty} \pi(x) = \infty.$$

Bereits Gauß hat eine Vermutung über das asymptotische Verhalten der Funktion  $\pi(x)$  ausgesprochen, nämlich

$$\pi(x) \sim \frac{x}{\log x}.$$

Dabei bedeutet das Zeichen  $\sim$  *asymptotisch gleich*, d.h. der Quotient der rechten und linken Seite konvergiert für  $x \rightarrow \infty$  gegen 1. Diese Vermutung wurde 1896 unabhängig von Hadamard und de la Vallée Poussin bewiesen. In dieser Vorlesung werden wir nur eine abgeschwächte Form des Primzahlsatzes beweisen, nämlich

$$c_1 \frac{x}{\log x} \leq \pi(x) \leq c_2 \frac{x}{\log x} \quad \text{für } x \geq x_0$$

mit gewissen Konstanten  $0 < c_1 < 1 < c_2$ . Solche Abschätzungen wurden zuerst von Tschebyscheff um 1850 bewiesen.

Wir benötigen einige Vorbereitungen.

**2.3. Lemma** (Legendre). *Für jede natürliche Zahl  $n$  und jede Primzahl  $p$  gilt*

$$\text{ord}_p(n!) = \sum_{k \geq 1} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

*Beweis.* Die Anzahl der Zahlen aus  $\{1, 2, \dots, n\}$ , die durch  $p$  teilbar sind, ist gleich  $\lfloor n/p \rfloor$ . Davon sind  $\lfloor n/p^2 \rfloor$  sogar durch  $p^2$  teilbar,  $\lfloor n/p^3 \rfloor$  durch  $p^3$ , usw. Daraus folgt die Behauptung.

**2.4. Lemma.** Sei  $n \geq 1$  eine natürliche Zahl. Für den Binomial-Koeffizienten  $\binom{2n}{n}$  gelten die folgenden Aussagen:

- a)  $2 \mid \binom{2n}{n}$  und  $p \mid \binom{2n}{n}$  für alle Primzahlen  $p$  mit  $n < p \leq 2n$ .
- b) Ist  $p \geq 3$  eine Primzahl mit  $2n/3 < p \leq n$ , so folgt  $p \nmid \binom{2n}{n}$ .
- c) Falls  $p^r \mid \binom{2n}{n}$  für eine Primzahlpotenz  $p^r$ , so folgt  $p^r \leq 2n$ .
- d)  $\frac{2^{2n-1}}{n} \leq \binom{2n}{n} \leq 2^{2n-1}$ .

*Beweis.* a) Es gilt

$$\binom{2n}{n} = \binom{2n-1}{n-1} + \binom{2n-1}{n} = 2 \binom{2n-1}{n-1} \implies 2 \mid \binom{2n}{n}$$

und

$$\binom{2n}{n} = \frac{2n \cdot (2n-1) \cdot \dots \cdot (n+1)}{1 \cdot 2 \cdot \dots \cdot n}.$$

Eine Primzahl  $n < p \leq 2n$  im Zähler kann sich deshalb nicht wegkürzen.

b) Da  $p^2 > 2n$  gilt nach Lemma 2.3

$$\text{ord}_p \binom{2n}{n} = \text{ord}_p \left( \frac{(2n)!}{(n!)^2} \right) = \left\lfloor \frac{2n}{p} \right\rfloor - 2 \left\lfloor \frac{n}{p} \right\rfloor = 2 - 2 = 0,$$

d.h.  $p \nmid \binom{2n}{n}$ .

c) In der Formel

$$\text{ord}_p \binom{2n}{n} = \sum_{k \geq 1} \left\{ \left\lfloor \frac{2n}{p^k} \right\rfloor - 2 \left\lfloor \frac{n}{p^k} \right\rfloor \right\}$$

ist jeder Summand entweder 0 oder 1, denn für jede reelle Zahl  $x$  gilt  $\lfloor 2x \rfloor - 2\lfloor x \rfloor \in \{0, 1\}$ . Da  $\lfloor 2n/p^k \rfloor = 0$  für

$$k > r_p := \left\lfloor \frac{\log 2n}{\log p} \right\rfloor$$

folgt  $\text{ord}_p \binom{2n}{n} \leq r_p$ , also  $p^r \leq p^{r_p} \leq 2n$ .

d) Aus  $(1 + 1)^{2n-1} = 2^{2n-1}$  folgt mit dem binomischen Lehrsatz

$$(*) \quad 1 + \binom{2n-1}{1} + \dots + \binom{2n-1}{n-1} + \binom{2n-1}{n} + \dots + \binom{2n-1}{2n-2} + 1 = 2^{2n-1}$$

Daraus folgt einerseits

$$\binom{2n}{n} = \binom{2n-1}{n-1} + \binom{2n-1}{n} \leq 2^{2n-1}$$

und andererseits, da  $\binom{2n-1}{n-1} = \binom{2n-1}{n}$  die größten der  $2n$  Summanden der linken Seite von (\*) sind,

$$\binom{2n-1}{n-1} = \binom{2n-1}{n} \geq \frac{2^{2n-1}}{2n},$$

also

$$\binom{2n}{n} \geq \frac{2^{2n-1}}{n}.$$

**2.5. Satz.** Für alle  $n \geq 3$  gilt

$$\frac{1}{2} \cdot \frac{n}{\log n} \leq \pi(n) \leq 2 \cdot \frac{n}{\log n}.$$

*Beweis*

**A. Abschätzung nach oben**

Wir bezeichnen mit

$$P(m, 2m) = \prod_{m < p \leq 2m} p$$

das Produkt aller Primzahlen  $p$  mit  $m < p \leq 2m$ . Da die Anzahl der Faktoren gleich  $\pi(2m) - \pi(m)$  ist, folgt

$$P(m, 2m) > m^{\pi(2m) - \pi(m)}.$$

Nach Lemma 2.4 gilt

$$2P(m, 2m) \leq \binom{2m}{m} \leq 2^{2m-1},$$

also folgt

$$m^{\pi(2m) - \pi(m)} < 2^{2m-2},$$

also nach Logarithmieren

$$\pi(2m) - \pi(m) > \frac{(2m-2)\log 2}{\log m}. \quad (1)$$

Wir beweisen jetzt die Abschätzung nach oben durch Induktion nach  $n$ . Durch direktes Nachprüfen überzeugt man sich, dass die Abschätzung für  $3 \leq n \leq 2^7 = 128$  richtig ist.

*Induktionsschritt.* Sei zunächst  $n = 2m - 1 > 2^7$  ungerade. Es gilt  $\pi(2m - 1) = \pi(2m)$ . Aus (1) folgt unter Benutzung der Induktionsvoraussetzung für  $\pi(m)$

$$\begin{aligned} \pi(2m - 1) &\leq \pi(m) + \frac{(2m-2)\log 2}{\log m} \\ &\leq \frac{2m + (2m-2)\log 2}{\log m} \\ &= \frac{2m(1 + \log 2) - 2\log 2}{\log m} \\ &\stackrel{!}{\leq} 2 \cdot \frac{2m-1}{\log(2m-1)}. \end{aligned}$$

Die Abschätzung an der Stelle  $\stackrel{!}{\leq}$  ist äquivalent mit

$$2m(1 + \log 2) - 2\log 2 \leq (4m - 2) \cdot \frac{\log m}{\log(2m-1)}$$

und dies wiederum ist gleichbedeutend mit

$$(1 + \log 2) - \frac{\log 2}{m} \leq \left(2 - \frac{1}{m}\right) \cdot \frac{\log m}{\log(2m-1)}$$

Diese Ungleichung folgt aber aus

$$1 + \log 2 \leq \left(2 - \frac{1}{m}\right) \cdot \frac{\log m}{\log(2m)} = \left(2 - \frac{1}{m}\right) \left(1 - \frac{\log 2}{\log(2m)}\right) \quad (2)$$

Die Gültigkeit von (2) folgt für  $2m \geq 2^7$  daraus, dass

$$\left(2 - \frac{1}{2^6}\right) \left(1 - \frac{\log 2}{\log(2^7)}\right) = \left(2 - \frac{1}{64}\right) \left(1 - \frac{1}{7}\right) = 1.7008928 \dots$$

und  $1 + \log 2 = 1.693147 \dots$

Für gerade  $n = 2m$  folgt die Abschätzung nach oben aus

$$\pi(2m) = \pi(2m - 1) \leq 2 \cdot \frac{2m-1}{\log(2m-1)} < 2 \cdot \frac{2m}{\log(2m)}.$$

## B. Abschätzung nach unten

Nach Lemma 2.4 c) gilt

$$\binom{2m}{m} = \prod_{p \leq 2m} p^{k_p} \quad \text{mit } p^{k_p} \leq 2m,$$

also

$$\binom{2m}{m} \leq (2m)^{\pi(2m)}.$$

Daraus folgt

$$(2m)^{\pi(2m)} \geq \frac{2^{2m}}{2m}$$

und durch Logarithmieren

$$\pi(2m) \geq \frac{2m \log 2}{\log 2m} - 1 = \frac{2m}{\log 2m} \left( \log 2 - \frac{\log 2m}{2m} \right).$$

Für  $2m \geq 16$  ist

$$\left( \log 2 - \frac{\log 2m}{2m} \right) \geq \left( \log 2 - \frac{\log 16}{16} \right) = 0.519860 \dots > \frac{1}{2},$$

Damit ist die Abschätzung nach unten für gerade  $n \geq 16$  bewiesen, für  $16 > n \geq 3$  prüft man sie direkt nach.

Für ungerade  $n = 2m - 1$  folgt die Abschätzung aus

$$\pi(2m - 1) = \pi(2m) \geq \frac{1}{2} \cdot 2m \log 2m > \frac{1}{2} \cdot (2m - 1) \log(2m - 1).$$

**2.6. Satz.** *Für jede ganze Zahl  $n \geq 1$  gilt*

$$\prod_{p \leq n} p < 4^n.$$

*Dabei ist das Produkt über alle Primzahlen  $p \leq n$  zu nehmen.*

*Beweis.* Sei  $P(n) := \prod_{p \leq n} p$ . Es ist also zu zeigen, dass  $P(n) < 4^n$  für alle  $n \geq 1$ . Dies beweisen wir durch Induktion nach  $n$ .

Die Behauptung ist offensichtlich wahr für  $n = 1, 2$ .

Für den *Induktionsschritt* nehmen wir an, dass  $n \geq 3$  und  $P(k) < 4^k$  für alle  $k < n$  und schließen daraus  $P(n) < 4^n$ . Dies ist trivial, falls  $n$  gerade, denn  $P(2m) = P(2m - 1)$ .

Sei also  $n$  ungerade,  $n = 2m - 1$ . Nach Lemma 2.4a) und 2.4d) gilt

$$2 \left( \prod_{m < p \leq 2m-1} p \right) \mid \binom{2m}{m} \implies \prod_{m < p \leq 2m-1} p \leq 2^{2m-2} = 4^{m-1}.$$

Da nach Induktionsvoraussetzung  $P(m) < 4^m$ , folgt

$$P(2m - 1) = P(m) \prod_{m < p \leq 2m-1} p < 4^m \cdot 4^{m-1} = 4^{2m-1}, \quad \text{q.e.d.}$$

**2.7. Satz** (Bertrandsches Postulat). *Zu jeder natürlichen Zahl  $n \geq 1$  gibt es wenigstens eine Primzahl  $p$  mit  $n < p \leq 2n$ .*

*Beweis.* Wir benutzen die Primfaktor-Zerlegung von

$$N := \binom{2n}{n}.$$

Ist  $n \geq 3$ , so kommen nach Lemma 2.4a) und 2.4b) in  $N$  nur Primfaktoren  $p$  mit  $p \leq 2n/3$  und  $n < p \leq 2n$  vor. Nach 2.4c) ist die Vielfachheit jedes Primfaktors  $p \mid N$  mit  $p > \sqrt{2n}$  gleich 1. Wir führen folgende Abkürzungen ein:

$$P(2n/3) := \prod_{p \leq 2n/3} p, \quad P(n, 2n) := \prod_{n < p \leq 2n} p$$

und

$$Q := \prod_{p \leq \sqrt{2n}} p^{\text{ord}_p(N)-1}.$$

Damit gilt

$$\binom{2n}{n} \leq Q \cdot P(2n/3) \cdot P(n, 2n)$$

Um  $Q$  abzuschätzen, beachten wir, dass nach 2.4c)

$$p^{\text{ord}_p(N)} \leq 2n \implies p^{\text{ord}_p(N)-1} \leq n.$$

Die Anzahl der Primzahlen  $p \leq \sqrt{2n}$  ist  $\leq \sqrt{2n} - 1$ , also

$$Q \leq n^{\sqrt{2n}-1}.$$

Nach Lemma 2.6 ist  $P(2n/3) < 4^{2n/3} = 2^{4n/3}$ . Mit Lemma 2.4d) zusammen ergibt sich

$$\frac{2^{2n-1}}{n} \leq \binom{2n}{n} < n^{\sqrt{2n}-1} 2^{4n/3} P(n, 2n),$$

woraus folgt

$$P(n, 2n) > \frac{2^{2n/3-1}}{n\sqrt{2n}}.$$

Der Zähler wächst für  $n \rightarrow \infty$  schneller gegen  $\infty$ , als der Nenner; daher gibt es ein  $n_0$  mit  $P(n, 2n) > 1$  für  $n \geq n_0$ . Man kann  $n_0 = 2^9 = 512$  wählen, denn für  $n = 2^\alpha$  ist

$$\log\left(\frac{2^{2n/3-1}}{n\sqrt{2n}}\right) = \left(\frac{2n}{3} - 1\right) \log 2 - \sqrt{2n} \log n = \left(\frac{2^{\alpha+1}}{3} - 1 - 2^{(\alpha+1)/2} \alpha\right) \log 2.$$

Dies ist positiv für  $\alpha \geq 9$ . Also gilt  $P(n, 2n) > 1$  für  $n \geq 512$ , d.h. das Bertrandsche Postulat ist richtig für  $n \geq 512$ . Für kleinere  $n$  gilt es ebenfalls, wie die Reihe der Primzahlen

$$2, 3, 5, 7, 13, 23, 41, 71, 139, 263, 521$$

zeigt, von denen jede kleiner als das Doppelte der vorhergehenden ist.