2. Verteilung der Primzahlen. Bertrands Postulat

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

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

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

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 $x \geqslant 0$ bezeichnen wir mit $\pi(x)$ die Anzahl aller Primzahlen $p \leqslant x$. 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

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

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 $x \to \infty$ 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

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

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*

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

Bemerkung. Die Summe ist natürlich endlich, denn $\lfloor n/p^k \rfloor = 0$ für $p^k > n$.

Beweis. Die Anzahl der Zahlen aus $\{1, 2, \ldots, n\}$, die durch p teibar 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 $n \geqslant 1$ eine natürliche Zahl. Für den Binomial-Koeffizienten $\binom{2n}{n}$ gelten die folgenden Aussagen:*

a) $2 \,\Big|\, \binom{2n}{n}$ *und* $p \,\Big|\, \binom{2n}{n}$ *für alle Primzahlen p mit $n < p \leqslant 2n$.*

b) *Ist $p \geqslant 3$ eine Primzahl mit $2n/3 < p \leqslant n$, so folgt $p \nmid \binom{2n}{n}$.*

c) *Falls $p^r \,\Big|\, \binom{2n}{n}$ für eine Primzahlpotenz p^r, so folgt $p^r \leqslant 2n$.*

d) $\dfrac{2^{2n-1}}{n} \leqslant \binom{2n}{n} \leqslant 2^{2n-1}$.

Beweis. a) Es gilt

$$\binom{2n}{n} = \binom{2n-1}{n-1} + \binom{2n-1}{n} = 2\binom{2n-1}{n-1} \quad \Longrightarrow \quad 2 \,\Big|\, \binom{2n}{n}$$

und

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

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

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

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

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

c) In der Formel

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

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 $\operatorname{ord}_p\binom{2n}{n} \leqslant r_p$, also $p^r \leqslant p^{r_p} \leqslant 2n$.

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

$$(*) \qquad 1 + \binom{2n-1}{1} + \ldots + \binom{2n-1}{n-1} + \binom{2n-1}{n} + \ldots + \binom{2n-1}{2n-2} + 1 = 2^{2n-1}$$

Daraus folgt einerseits

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

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

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

also

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

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

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

Beweis

A. Abschätzung nach oben

Wir bezeichnen mit

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

das Produkt aller Primzahlen p mit $m < p \leqslant 2m$. 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 für $m \geqslant 2$

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

also folgt

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

und nach Logarithmieren

$$\pi(2m) - \pi(m) < \frac{(2m-2)\log 2}{\log m}. \tag{1}$$

Wir beweisen jetzt die Abschätzung nach oben durch Induktion nach n. Durch direktes Nachprüfen überzeugt man sich, dass die Abschätzung für $3 \leqslant n \leqslant 2^7 = 128$ 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 $\pi(m)$

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

Die Abschätzung an der Stelle $\overset{!}{\leqslant}$ ist äquivalent mit

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

und dies wiederum ist gleichbedeutend mit

$$(1+\log 2) - \frac{\log 2}{m} \;\leqslant\; \Big(2 - \frac{1}{m}\Big) \cdot \frac{\log m}{\log(2m-1)}.$$

Diese Ungleichung folgt aber aus

$$1 + \log 2 \leqslant \Big(2 - \frac{1}{m}\Big) \cdot \frac{\log m}{\log(2m)} = \Big(2 - \frac{1}{m}\Big)\Big(1 - \frac{\log 2}{\log(2m)}\Big) \tag{2}$$

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

$$\Big(2 - \frac{1}{2^6}\Big)\Big(1 - \frac{\log 2}{\log(2^7)}\Big) = \Big(2 - \frac{1}{64}\Big)\Big(1 - \frac{1}{7}\Big) = 1.7008928\ldots$$

und $1 + \log 2 = 1.693147\ldots$.

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

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

denn die Funktion $x \mapsto x/\log x$ ist streng monoton wachsend.

B. Abschätzung nach unten

Nach Lemma 2.4 c) gilt

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

also

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

Daraus folgt

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

und durch Logarithmieren

$$\pi(2m) \geqslant \frac{2m \log 2}{\log 2m} - 1 = \frac{2m}{\log 2m}\Big(\log 2 - \frac{\log 2m}{2m}\Big).$$

Für $2m \geqslant 16$ ist

$$(\log 2 - \frac{\log 2m}{2m}\Big) \geqslant (\log 2 - \frac{\log 16}{16}\Big) = 0.519860\ldots > \frac{1}{2},$$

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

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

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

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

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

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

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

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

Für den *Induktionsschritt* nehmen wir an, dass $n \geqslant 3$ 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

$$2\Big(\prod_{m<p\leqslant 2m-1} p\Big) \,\Big|\, \binom{2m}{m} \quad\Longrightarrow\quad \prod_{m<p\leqslant 2m-1} p \;\leqslant 2^{2m-2} = 4^{m-1}.$$

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

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

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

Beweis. Wir benutzen die Primfaktor-Zerlegung von

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

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

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

und

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

Damit gilt

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

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

$$p^{\operatorname{ord}_p(N)} \leqslant 2n \quad\Longrightarrow\quad p^{\operatorname{ord}_p(N)-1} \leqslant n.$$

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

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

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

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

woraus folgt

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

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

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

Dies ist positiv für $\alpha \geqslant 9$. Also gilt $P(n,2n) > 1$ für $n \geqslant 512$, d.h. das Bertrandsche Postulat ist richtig für $n \geqslant 512$. 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.