§4. Die Menge der Primzahlen. Bertrands Postulat

4.1. 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 gibt, die von allen p_j, $(1 \leqslant j \leqslant n)$, verschieden ist. Dazu bilden wir das Produkt

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

Dann ist N entweder selbst eine Primzahl oder besitzt einen Primfaktor, der von allen p_j verschieden ist, da $p_j \nmid N$ für alle j.

4.2. Mersennesche Primzahlen. *Eine ganze Zahl der Gestalt*

$$2^n - 1, \quad n \in \mathbb{N}_1 ,$$

ist höchstens dann eine Primzahl, wenn n eine Primzahl ist.

Beweis. Wir verwenden die bekannte Formel

$$x^n - 1 = (x-1)(x^{n-1} + x^{n-1} + \ldots + x + 1).$$

Ist $n = k\ell$, $k, \ell \geqslant 2$, keine Primzahl, so ist auch

$$2^n - 1 = (2^k)^\ell - 1 = (2^k - 1)(2^{k(\ell-1)} + \ldots + 1)$$

eine zusammengesetzte Zahl.

Die Zahlen

$$M_p := 2^p - 1, \quad p \text{ prim},$$

heißen *Mersennesche Zahlen*. Sie sind nicht alle prim. Die ersten Mersenneschen Primzahlen sind

$$\begin{aligned}
M_2 &= 2^2 - 1 = 3,\\
M_3 &= 2^3 - 1 = 7,\\
M_5 &= 2^5 - 1 = 31,\\
M_7 &= 2^7 - 1 = 127,\\
M_{13} &= 2^{13} - 1 = 8191,\\
M_{17} &= 2^{17} - 1 = 131071,\\
M_{19} &= 2^{19} - 1 = 524287,\\
M_{31} &= 2^{31} - 1 = 2147483647.
\end{aligned}$$

Dagegen sind

$$M_{13} = 2^{11} - 1 = 2047 = 23 \cdot 89,$$
$$M_{17} = 2^{23} - 1 = 8388607 = 47 \cdot 178481,$$
$$M_{29} = 2^{29} - 1 = 536870911 = 233 \cdot 1103 \cdot 2089$$

zusammengesetzt. Die größte bekannte Primzahl, deren Primalität noch ohne Computer bewiesen wurde (von Lucas 1876), war

$$M_{127} = 1701\ 41183\ 46046\ 92317\ 31687\ 30371\ 58841\ 05727.$$

Seit Dezember 2003 ist die größte bekannte Primzahl M_p mit $p = 20\,996\,011$. Diese Zahl hat über 6 Millionen Dezimalstellen. Es ist dies erst die 40-te bekannte Mersennesche Primzahl. Es wird vermutet, ist aber nicht bewiesen, dass es unendlich viele Mersennesche Primzahlen gibt. Wir werden später einen effizienten Primzahltest für Mersennesche Zahlen behandeln.

4.3. Fermatsche Primzahlen. *Eine ganze Zahl der Gestalt*

$$2^N + 1, \quad N \in \mathbb{N}_1\,,$$

ist höchstens dann eine Primzahl, wenn $N = 2^n$ eine Zweierpotenz ist.

Beweis. Für ungerades n gilt die Formel

$$x^n + 1 = (x+1)(x^{n-1} - x^{n-1} + - \ldots - x + 1),$$

die sich aus der in 4.2 verwendeten Formel durch die Substitution $x \to -x$ und Multiplikation mit -1 ergibt. Ist N keine Zweierpotenz, so kann man schreiben $N = 2^k u$ mit einer ungeraden ganzen Zahl $u \geqslant 3$. Dann ist

$$2^N + 1 = (2^{2^k})^u + 1 = (2^{2^k} + 1)(2^{2^k(u-1)} - + \ldots - 2^{2^k} + 1)$$

eine zusammengestzte Zahl.

Man nennt

$$F_n := 2^{2^n} + 1$$

eine Fermatsche Zahl. Fermat hatte behauptet, dass alle F_n prim seien. Zwar sind

$$F_0 = 2^1 + 1 = 3,$$
$$F_1 = 2^2 + 1 = 5,$$
$$F_2 = 2^4 + 1 = 17,$$
$$F_3 = 2^8 + 1 = 257,$$
$$F_4 = 2^{16} + 1 = 65537$$

prim, aber bereits Euler stellte fest, dass

$$F_5 = 2^{32} + 1 = 42949\ 67297 = 641 \cdot 6700417$$

zusammengesetzt ist. Außer $F_0, \ldots, F_4$ sind keine weiteren Fermatschen Primzahlen bekannt. Von vielen Fermatzahlen weiß man, dass sie zusammengesetzt sind. Wir werden später noch einmal auf die Fermatzahlen zurückkommen.

4.4. Lemma. *Für jede natürliche Zahl n und jede Primzahl p gilt*

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

Beweis. ...

4.5. Lemma. *Sei $n \geqslant 1$ 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 $n < p \leqslant 2n$.*

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

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

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

Beweis. ...

4.6. Satz. *Für jede natürliche Zahl n 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 $n \leqslant 2$.

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 $P(2m-1) = P(2m)$. Sei also n ungerade, $n = 2m - 1$. Nach Lemma 4.5a) und 4.5d) 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

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

4.7. Satz (Bertrands 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 4.5a) und 4.5b) in N nur Primfaktoren p mit $p \leqslant 2n/3$ und $n < p \leqslant 2n$ vor. Nach 4.5c) 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 4.5c)

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

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

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

Nach Lemma 4.6 ist $P(2n/3) < 4^{2n/3} = 2^{4n/3}$. Mit Lemma 4.5d) 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

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

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.

4.8. Der Primzahlsatz. Für eine positive reelle Zahl x bezeichnen wir mit $\pi(x)$ die Anzahl aller Primzahlen $\leqslant x$. Es ist also z.B.

$$\pi(1) = \pi(\sqrt{2}) = 0, \quad \pi(2) = 1, \quad \pi(4) = 2, \quad \pi(10) = 4.$$

Der Primzahlsatz macht eine Aussage über das asymptotische Verhalten von $\pi(x)$ für $x \to \infty$. Die Aussage ist

$$\pi(x) \sim \frac{x}{\log x} \quad \text{für } x \to \infty.$$

Dabei bedeutet das Zeichen $\sim$ "*asymptotisch gleich*"; man setzt $f(x) \sim g(x)$, wenn $g(x) \neq 0$ für $x \geqslant x_0$ und

$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1.$$

Der Primzahlsatz wurde von Gauß vermutet und 1896 unabhängig von Hadamard und de la Vallée Poussin bewiesen. Der Beweis benutzt Hilfsmittel der Analytischen Zahlentheorie; wir werden ihn in dieser Vorlesung nicht ausführen.