Primzahlen

Stilianos Louca

28. Februar 2009

---

1 Primzahlen

1.0.1 Definition: Definition: Primzahl

Eine Zahl $p \in \mathbb{N} \setminus \{1\}$ ist genau dann eine Primzahl wenn folgendes gilt:

$$\forall\, n \in \mathbb{N} \quad : \quad \frac{p}{n} \in \mathbb{N} \;\Rightarrow\; (n = 1) \vee (n = p)$$

Bemerkungen:

- Definitionsgemäß ist 1 keine Primzahl.
- Die ersten 5 Primzahlen sind 2,3,5,7,11.
- Alle geraden Zahlen größer als 2 sind keine Primzahlen.
- Die Menge aller Primzahlen ist $\mathbb{P}$.
- Man nennt zwei Zahlen $a, b \in \mathbb{Z}$ *prim zu einander*, falls gilt

$$\nexists\, n \in \mathbb{Z} \setminus \{\pm 1\} : \frac{a}{n} \in \mathbb{Z} \;\wedge\; \frac{b}{n} \in \mathbb{Z}$$

1.1 Jede natürliche Zahl größer als 1 kann in Primfaktoren zerlegt werden

Sei $M := \{m \in \mathbb{N} \;|\; \exists\, p_1, p_2, ..., p_k \in \mathbb{P} : m = p_1 \cdot p_2 \cdot ... \cdot p_k\}$.
Offensichtlich gilt:

$$a, b \in M \;\Rightarrow\; a \cdot b \in M$$

Behauptung: $M = \mathbb{N} \setminus \{1\}$

Beweis

Induktionsanfang: Für $n = 2$ klar, da $2 \in \mathbb{P}$.
Induktionsannahme: $\{2, 3, .., n\} \subset M$ für irgendein $n \in \mathbb{N} \setminus \{1\}$.
Induktionsschritt: Sei $m = n + 1$. Dann ist zwischen zwei Fällen zu unterscheiden:

- Fall 1: $\exists\, a \in \{2, .., m-1\} \;:\; \underbrace{\frac{m}{a}}_{\leq n} \in \mathbb{N}$. Doch wegen $a \in M$ ist auch $m = a \cdot \frac{m}{a} \in M$.
- Fall 2: $\nexists\, a \in \{2, .., m-1\} : \frac{m}{a} \in \mathbb{N}$. Doch dies bedeutet genau $m \in \mathbb{P} \subset M$.

□

Bemerkung: Somit folgt insbesondere für Zahl $a \in \mathbb{N} \setminus \{1\}$:

$$\left(\forall\, p \in \mathbb{P} \setminus \{a\} : \frac{a}{p} \notin \mathbb{N}\right) \;\Rightarrow\; a \in \mathbb{P}$$

1.2 Es gibt unendlich viele Primzahlen

$$\forall\, p_1 \in \mathbb{P} \;:\; \exists\, p_2 \in \mathbb{P} : p_2 > p_1$$

Beweis durch Widerspruch

Annahme: $\mathbb{P}$ ist endlich. Dann sei $\lambda := \prod_{p_i \in \mathbb{P}} p_i$ und $p := \lambda - 1$. Dann gilt:

$$\forall\, p_i \in \mathbb{P} : \frac{p}{p_i} = \underbrace{\frac{\lambda}{p_i}}_{\in \mathbb{N}} - \underbrace{\frac{1}{p_i}}_{\notin \mathbb{N}} \notin \mathbb{N}$$

das heißt nach obiger Bemerkung $p \in \mathbb{P}$. Doch $p > \max \mathbb{P}$ (da $\lambda > 2 \cdot \max \mathbb{P}$), was ein Widerspruch ist!
□

1.3 Die Wurzel einer nicht-quadratischen Zahl ist immer Irrational

Es sei $p \in \mathbb{N}$ nicht-quadratisch, das heißt $\sqrt{p} \notin \mathbb{N}$. Dann gilt sogar $\sqrt{p} \notin \mathbb{Q}$.
Spezialfall: Primzahlen sind nicht-quadratisch.

Beweis durch Widerspruch

Sei $p \in \mathbb{N}$ und $\sqrt{p} \in \mathbb{Q}$. Dann

$$\exists\, a, b \in \mathbb{N} \;:\; \sqrt{p} = \frac{a}{b}$$

mit a, b prim zu einander. Da auch $a \cdot a$ und $b \cdot b$ prim zu einander sind, folgt aus

$$p = \frac{a \cdot a}{b \cdot b}$$

und $p \in \mathbb{N}$ notwendigerweise[1] $b \cdot b = 1$, also $p = a \cdot a$, das heißt p ist quadratisch.
□

1.4 Der Abstand zwischen zwei aufeinander folgenden Primzahlen kann beliebig groß werden

Sei p_n die n-te Primzahl nach Größenordnung. Dann gilt:

$$\forall\, m \in \mathbb{N} : \exists\, p_n \in \mathbb{P} : (p_{n+1} \geq p_n + m)$$

Beweis

Es sei $m \in \mathbb{N}$ beliebig. Dann gilt:

$$\forall\, k \in \mathbb{N} \cap [2, m] : \frac{m! + k}{k} = \frac{m!}{k} + 1 \in \mathbb{N} \Rightarrow\; (m! + k) \notin \mathbb{P}$$

Sei nun

$$p_n := \max \{p \in \mathbb{P} : p \leq m! + 1\}$$

Dann ist

$$p_{n+1} \geq m! + m + 1 \geq p_n + m$$

□

[1] Denn $\frac{aa}{bb} \in \mathbb{N} \;\wedge\; \frac{bb}{bb} \in \mathbb{N}$