§ 5. Primzahlen

Jede ganze Zahl a besitzt die sog. **trivialen** oder **unechten** Teiler ± 1 und $\pm a$. Davon verschiedene Teiler von a heißen **echt** oder **nichttrivial**. Primzahlen sind Zahlen ohne echte Teiler, genauer

(5.1) DEF: Eine natürliche Zahl $p \in \mathbb{N}$ heißt **Primzahl** oder **prim**, wenn gilt:

P_1) $p \geq 2$

P_2) 1 und p sind die einzigen positiven Teiler von p.

$\mathbb{P}$ bezeichne die **Menge aller Primzahlen**.

Beispiele: $\{2, 3, 5, 7, 11, 13\} \subseteq \mathbb{P}$

$1 \notin \mathbb{P}$, $4 \notin \mathbb{P}$, $6 \notin \mathbb{P}$, $-2 \notin \mathbb{P}$, $-3 \notin \mathbb{P}$, $-13 \notin \mathbb{P}$

(5.2) BEM: **a)** 1 ist keine Primzahl !!!

b) Eine natürliche Zahl $p \geq 2$ ist genau dann eine Primzahl, wenn gilt

$$\forall\, t \in \mathbb{N} \,:\, t \,|\, p \implies t = 1 \,\vee\, t = p\,.$$

c) Eine natürliche Zahl $n \geq 2$ ist genau dann keine Primzahl, wenn n einen echten Teiler besitzt, d.h. wenn es ein

$$t \in \mathbb{N} \text{ mit } 1 < t < n \text{ und } t \,|\, n$$

gibt. In dem Falle ist dann auch der zu t komplementäre Teiler s ein echter Teiler von n. Also

$$n \in \mathbb{N}, n \geq 2 \,:\, n \notin \mathbb{P} \iff \text{es gibt } s, t \in \mathbb{N} \text{ mit } 1 < s, t < n \text{ und } n = s \cdot t\,.$$

d) Eine natürliche Zahl, die einen echten Teiler besitzt, heißt eine **zusammengesetzte** Zahl. Es gilt also

$$\mathbb{N} \;=\; \{1\} \cup \mathbb{P} \cup M\,,$$

wobei M die Menge der zusammengesetzten natürlichen Zahlen bezeichnet.

e) 2 ist die einzige gerade Primzahl, alle anderen Primzahlen sind ungerade.

f) Für $n \in \mathbb{N}$ gilt: n prim $\iff$ $|\, T^+(n)\,| = 2$ $\iff$ $|\, T(n)\,| = 4$.

(5.3) LEMMA: Für $a \in \mathbb{Z}$ und $p \in \mathbb{P}$ gilt:

a) $\mathrm{ggT}(a, p) \in \{1, p\}$

b) $\mathrm{ggT}(a, p) = p \iff p \,|\, a$

c) $\mathrm{ggT}(a, p) = 1 \iff p \nmid a$.

(5.4) SATZ: Für $p \in \mathbb{N}$, $p \geq 2$ sind folgende Aussagen äquivalent:

a) p ist eine Primzahl

b) $\forall\, a, b \in \mathbb{Z} :\; p \,|\, (a \cdot b) \implies (p \,|\, a \,\vee\, p \,|\, b)$.

(5.5) BEM: Wir haben gesehen, daß Primzahlen zwei zueinander äquivalente Bedingungen erfüllen. Eine natürliche Zahl $p \geq 2$ ist genau dann eine Primzahl, wenn

$$\forall\, t \in \mathbb{N} \,:\, t \,|\, p \quad \Longrightarrow \quad t = 1 \,\vee\, t = p$$

oder

$$\forall\, a, b \in \mathbb{Z} \,:\, p \,|\, (a \cdot b) \quad \Longrightarrow \quad p \,|\, a \,\vee\, p \,|\, b\,.$$

gilt. Im ersten Falle sagen wir, daß p **unzerlegbar** ist: p läßt sich nicht in ein Produkt echter Teiler zerlegen. Die zweite Eigenschaft wollen wir zur Unterscheidung die **Primeigenschaft** von p nennen. In späteren Verallgemeinerungen werden wir sehen, daß diese beiden Bedingungen nicht mehr übereinstimmen müssen.

(5.6) SATZ: Sei $n \in \mathbb{N}$, $n \geq 2$. Dann gilt:

a) Es gibt unter allen Teilern von n, die > 1 sind, einen kleinsten Teiler p

b) Dieser kleinste Teiler p ist eine Primzahl, also ein **Primteiler** von n.

c) n läßt sich als ein Produkt von endlich vielen Primzahlen darstellen.

Verteilung der Primzahlen

Mit Hilfe des Satzes (5.6) können wir jetzt mit Ideen, die schon in den Elementen des Euklid zu finden sind, beweisen, daß es unendlich viele Primzahlen gibt. Wir werden später noch weitere Beweise für dieses Ergebnis kennenlernen.

(5.7) SATZ: (Euklid)

Ist $\mathbb{P}' \subseteq \mathbb{P}$ eine endliche Menge von Primzahlen, so gibt es eine Primzahl p, die nicht in $\mathbb{P}'$ liegt (d.h. $\mathbb{P} \setminus \mathbb{P}' \neq \emptyset$).

(5.8) KOROLLAR: Es gibt unendlich viele Primzahlen (**I. Beweis**).

(5.9) KOROLLAR: Ist $(p_k)_{k\in\mathbb{N}}$ die Folge der Primzahlen in ihrer natürlichen Reihenfolge, so gilt

$$p_{n+1} \;<\; p_n^n + 1\,.$$

(5.10) KOROLLAR: Ist $(p_k)_{k\in\mathbb{N}}$ die Folge der Primzahlen in ihrer natürlichen Reihenfolge, so gilt

$$p_n \;<\; 2^{2^n}\,.$$

(5.11) DEF: Eine natürliche Zahl F_n $(n \in \mathbb{N}_0)$ der Form $F_n \;=\; 2^{2^n} + 1$ heißt ***n*–te Fermat'sche Zahl**.

Die Fermat'schen Zahlen F_0, F_1, F_2, F_3, F_4 sind Primzahlen, weitere Fermat'sche Primzahlen sind nicht bekannt.

Ungelöstes Problem: Gibt es unendlich viele Fermat'sche Primzahlen ???

(5.12) SATZ: Für alle $m, n \in \mathbb{N}_0$ mit $m \neq n$ gilt $\operatorname{ggT}(F_m, F_n) \;=\; 1\,.$

(5.13) KOROLLAR: Es gibt unendlich viele Primzahlen (**II. Beweis**).

(5.14) DEF: Ein Zahlenpaar $(p, p+2)$, bei dem sowohl p als auch $p+2$ Primzahlen sind, heißt ein **Primzahlzwilling**.

Beispiele: für Primzahlzwillinge: $(3,5)$, $(5,7)$, $(11,13)$, $(17,19)$, $(29,31)$,

$(q, q+2)$ mit $q = 242\,206\,083 \cdot 2^{38\,880} - 1$ (q hat 11 713 Dezimalziffern).

Das letzte Beispiel wurde 1995 von Indlekofer/Jarai/Wassing hier in Paderborn gefunden und war damals der größte bekannte Primzahlzwilling (jetzt gibt es aber schon viel größere!).

Ungelöstes Problem: Gibt es unendlich viele Primzahlzwillinge ???

(5.15) SATZ: Zu jeder natürlichen Zahl n gibt es n aufeinanderfolgende zusammengesetzte Zahlen.

(5.16) KOROLLAR: Ist $(p_k)_{k\in\mathbb{N}}$ die Folge der Primzahlen in ihrer natürlichen Reihenfolge, so gibt es zu jedem $n \in \mathbb{N}$ ein $m \in \mathbb{N}$ mit

$$p_{m+1} - p_m \;\geq\; n$$

(5.17) BEM: **a)** Ist $n \in \mathbb{N}$, $n \geq 3$, so gibt es mindestens eine Primzahl p mit

$$n \;<\; p \;\leq n! - 1\,.$$

b) **"Bertrand'sches Postulat"** (1845), bewiesen von Tschebyscheff

Zu jeder natürlichen Zahl n gibt es eine Primzahl p mit

$$n \;<\; p \;\leq\; 2n\,.$$

(5.18) SATZ: Ist $f \in \mathbb{Z}[T]$ ein nichtkonstantes Polynom, so ist $f(n)$ für unendlich viele $n \in \mathbb{N}$ eine zusammengesetzte Zahl (d.h. keine Primzahl).

Fazit: Es gibt kein nichtkonstantes Polynom $f \in \mathbb{Z}[T]$ mit der Eigenschaft: $f(n) \in \mathbb{P}$ für fast alle $n \in \mathbb{N}$.

(5.19) LEMMA:

a) Für jede ungerade Primzahl $p \in \mathbb{P}$ gilt: $p \bmod 4 = 1$ oder $p \bmod 4 = 3$

b) Für jede Primzahl $p \geq 5$ gilt: $p \bmod 6 = 1$ oder $p \bmod 6 = 5$.

(5.20) KOROLLAR:

a) Für jede ungerade Primzahl $p \in \mathbb{P}$ gibt es ein $k \in \mathbb{N}$ mit $p = 4k \pm 1$.

b) Für jede Primzahl $p \geq 5$ gibt es ein $l \in \mathbb{N}$ mit $p = 6l \pm 1$.

(5.21) SATZ: Es gibt unendlich viele Primzahlen der Form $4n+3$ ($n \in \mathbb{N}$).

(5.22) SATZ: Dirichlet (1837)

Sei $n \in \mathbb{N}$. Sind $a, b \in \mathbb{N}$ teilerfremd mit $0 < b < a$, so gibt es in der "arithmetischen Progression" $(an + b)_{n\in\mathbb{N}}$ unendlich viele Primzahlen.

Primzahltest:

(5.23) SATZ: Für eine natürliche Zahl $n \geq 2$ sind folgende Aussagen äquivalent:

a) n ist eine Primzahl

b) n besitzt keinen Teiler $t \in \mathbb{N}$ mit $2 \leq t \leq \lfloor\sqrt{n}\rfloor$

c) n besitzt keinen Primteiler p mit $p \leq \lfloor\sqrt{n}\rfloor$.

(5.24) Ein einfacher Primzahltest

Sei $n \geq 7$ eine ungerade Zahl. $(u_k)_{k\in\mathbb{N}}$ sei eine streng monoton wachsende Folge ungerader natürlicher Zahlen, die alle ungeraden Primzahlen enthält. Dann gilt

$$n \in \mathbb{P} \iff \forall\, k \in \mathbb{N} : u_k \leq \lfloor\sqrt{n}\rfloor \implies u_k \nmid n\,.$$

(5.25) BEISPIELE: Für die Folge (u_k) in (5.24) kann man wählen:

a) Die Folge aller ungeraden natürlichen Zahlen ≥ 3

$$3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31, 33, 35, 37, \ldots$$

b) 3 und dann die Zahlen $6k - 1, 6k + 1$ $(k \in \mathbb{N})$

$$3, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35, 37, \ldots$$

(Diese Folge enthält nach (5.20b) alle ungeraden Primzahlen)

c) Die Folge aller ungeraden Primzahlen in der natürlichen Reihenfolge

$$3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, \ldots.$$

Primzahllisten:

(5.26) Das Sieb des Eratosthenes

Sei $n \in \mathbb{N}$. Es sollen alle Primzahlen $\leq n$ bestimmt werden.

Sei $U = (3, 5, 7, 9, 11, \ldots)$ die Folge der ungeraden Zahlen $\leq n$ in der natürlichen Reihenfolge.

a) Streiche in U alle echten Vielfachen von 3.

b) Ist a die nächste ungestrichene Zahl, so brich das Verfahren im Falle $a > \lfloor\sqrt{n}\rfloor$ ab, ansonsten streiche die echten Vielfachen von a.

c) Setze das Verfahren fort, bis die nächste ungestrichene Zahl $> \lfloor\sqrt{n}\rfloor$ ist.

Es bleiben dann alle Primzahlen $\leq n$ übrig.