



more: bigdev.de/teaching

Primzahl-Klassiker

Primzahl-Klassiker - Hauptsatz elementare ZT

Hauptsatz der elementaren Zahlentheorie

Jede natürliche Zahl $n \geq 2$ besitzt eine (bis auf die Faktoreihenfolge) eindeutige PFS.

Wir brauchen zum Beweis die folgende Aussage:

Satz vom kleinsten Teiler.

Sei $n \in \mathbb{N} \setminus \{1\}$. Der kleinste Teiler $d \in \mathbb{N}$ mit $d > 1$ von n ist eine Primzahl

Beweis. $T(n) \setminus \{1\}$ ist nicht leer weil $n \in T(n)$

Dann gibt es nach dem Wohlordnungsprinzip eine kleinste Zahl in $T(n) \setminus \{1\}$. Diese sei d

Zeige $d \in P$

Annahme $d \notin P$

Dann existieren $a, b \in \mathbb{N} \setminus \{1; d\}$: $a \cdot b = d$ $a, b < d$

$\Rightarrow a | d$ außerdem $d | n$

$\Rightarrow a | n$ mit $a < d$ und $d < n \Rightarrow a < n$

$\Rightarrow d$ kann nicht das kleinste Element in $T(n) \setminus \{1\}$ gewesen sein

$\Rightarrow d \in P$ ✓

Beweis der Existenz des PFZ. Sei $n \in \mathbb{N} \setminus \{1\}$.

Fall 1: $n \in \mathbb{P}$. $n \in \mathbb{P}$

Fall 2: $n \notin \mathbb{P}$. $\Rightarrow \exists d_1, q_1 \in \mathbb{N} \setminus \mathbb{EFG}$ mit $d_1 \cdot q_1 = n$
und d_1 ist das kleinste Element in
 $T(q_1) \setminus \mathbb{EFG}$, also $d_1 \in \mathbb{P}$

Betrachte q_1

Fall 1 $q_1 \in \mathbb{P}$ Dann ist $n = d_1 \cdot q_1$ PFZ von n

Fall 2 $q_1 \notin \mathbb{P}$ Dann verfahren für oben

$$d_1 \cdot d_2 \cdot q_2 = q_1$$

Beweis der Eindeutigkeit der PFZ. Sei n die kleinste natürliche

Zahl mit mehr als einer PFZ:

$$n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots + q_e \quad (p_i, q_j \in \mathbb{P})$$

p_i und q_j paarweise verschieben

ohne Beschränkung der Allgemeinheit nehmen wir an $p_1 < q_1$

$$\alpha = n/p_1 = p_2 \cdots p_k$$

$$\beta = n/q_1 = q_2 \cdots q_e$$

$$\gamma = n - p_1 \cdot \beta \quad 0 < \gamma < n$$

α, β, γ haben eindeutige PFZ

$$\gamma = n - p_1 \cdot \beta = p_1 \cdot \alpha - p_1 \cdot \beta = p_1(\alpha - \beta)$$

$$\gamma = n - p_1 \cdot \beta = q_1 \cdot \beta - p_1 \cdot \beta = (q_1 - p_1) \cdot \beta$$

$$p_1 \cdot (\alpha - \beta) = (q_1 - p_1) \cdot \beta \Rightarrow p_1((q_1 - p_1) \cdot \beta)$$

$$p_1 + b \Rightarrow p_1/q_1 - p_1$$

$$p_1/(q_1 - p_1) \geq p_1/p_1$$

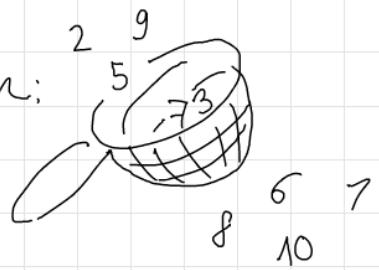
$$\Rightarrow p_1/(q_1 - p_1) + p_1$$

$$\Rightarrow p_1/q_1$$



Primzahl-Klassiker - Sieb des Eratosthenes

Wie findet man Primzahlen? Sieben:



2	3	4	5	6	7	8	9	10	
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50

Bis nach welcher Zahl muss ich sieben? 5

- 7
 11

Allgemein: Zum Sieben aller Primzahlen $\leq N$ muss ich bis nach der Zahl \sqrt{N} sieben.



Bestimmen Sie alle Primzahlen ≤ 100 .

$$n = 100 \quad \sqrt{n} = 10$$

2; 3; 5; 7; 11; 13; 17; 19; 23; 29; 31; 37; 41; 43; 53; 57; 59; 61; 67; 71; 73; 79; 83; 89; 97

Primzahl-Klassiker - Satz des Euklid

Wie viele Primzahlen gibt es? 2, 3, 5, 7, 11, 13, ...

Satz des Euklid. Es gibt unendlich viele Primzahlen.

Indirekter Beweis: Annahme: Es gibt endlich
viele Primzahlen $p_1, p_2, p_3, \dots, p_k$

$$\text{Sei } n = p_1 \cdot p_2 \cdot p_3 \cdots \cdot p_k + 1$$

Sei $p_i \in \mathbb{P}$ mit $p_i | n$

$$a | b \wedge a | c \rightarrow a | (b+c)$$

$$p_i | ((p_1 \cdot p_2 \cdots \cdot p_k) + 1) \wedge p_i | (p_1 \cdot p_2 \cdots \cdot p_k)$$

$$\Rightarrow p_i | ((p_1 \cdot p_2 \cdots \cdot p_k) + 1 - (p_1 \cdot p_2 \cdots \cdot p_k)) \Rightarrow p_i | 1$$