3.11.05

Satz Es gibt unendlich viele Primzahlen

Beweis: durch Widerspruch:

Annahme: Es gibt genau k Primzahlen

$p_1, p_2, \dots, p_k$ sei $p\# = p_1 p_2 \cdot \dots \cdot p_k > 1$

Wähle Primteiler p von $p\# + 1$. Es sei also $p\# + 1 = p \cdot q$

Da $p_1, \dots, p_k$ alle Primzahlen sind, gibt es

$j \in \{1, \dots, k\}$ mit $p = p_j$. Durch Umnummerierung

können wir $j = 1$ annehmen

$\Rightarrow 1 = p \cdot q - p\# = p_1 \cdot q - p_1 p_2 \cdot \dots \cdot p_k = p_1 (q - p_2 \cdot \dots \cdot p_k)$

$\Rightarrow p_1 = 1$ Widerspruch

Bemerkung: Primzahlpaare (p_1, p_2) mit $p_2 = p_1 + 2$ heißen Primzahlzwillinge. Offen ist die Frage, ob es unendlich viele Primzahlzwillinge gibt.

$m \mid n \Rightarrow m \leq n$

Division mit Rest

Seien $m, n \in \mathbb{N}$ mit $m \leq n$ und $m \neq n$ ($\Rightarrow 1 < m < n$) gegeben. Dann gibt es genau ein Paar $(q_1, r_1) \in \mathbb{N}^2$ mit

$n = m \cdot q_1 + r_1$, $r_1 < m$ r_1 Rest bei der Division von n durch m

Beweis: Eindeutigkeit. $n = m q_1 + r_1 = m q_2 + r_2$ $r_1, r_2 < m$

- 1. Fall: $r_1 = r_2 \Rightarrow m q_1 = m q_2 \Rightarrow q_1 = q_2$
- 2. Fall: O.B.d.A $r_1 < r_2$, $r_2 = r_1 + d$

$\Rightarrow m q_1 + r_1 = m q_2 + r_2 \Rightarrow m q_1 = m q_2 + d \Rightarrow m \mid d$

$\Rightarrow m \leq d < r_2$ Widerspruch

Existenz: Es sei $M = \{ q \in \mathbb{N} \mid mq > n \} \ni n$

$\neq 1$

setze $q_2 = \min M > 1 \Rightarrow q_2 - 1 = q_1 \notin M$

$\Rightarrow m \cdot q_1 < n$. Setze $r_1 = n - m q_1 \Rightarrow m \cdot q_1 + r = n <$

$< m \cdot q_2 = m \cdot (q_1 + 1) = m q_1 + m \Rightarrow r_1 < m$

q.e.d.

Jede streng monoton fallende Folge natürlicher Zahlen bricht ab.

Euklidischer Algorithmus

$m, n \in \mathbb{N}, \quad m \leq n, \quad m \nmid n$

$n = m \cdot q_1 + r_1 \qquad r_1 < m$

$m = r_1 \cdot q_2 + r_2 \qquad r_2 < r_1$

$r_1 = r_2 \cdot q_3 + r_3 \qquad r_3 < r_2$

$\vdots$

$r_k = r_{k+1} \cdot q_{k+2} + r_{k+2} \qquad r_{k+2} < r_{k+1}$

$r_{k+1} = (r_{k+2}) \, q_k$

$\Rightarrow r_{k+2}$ ist gemeinsamer Teiler von m und n.

Jeder gemeinsamer Teiler t von m und n ist Teiler von r_{k+2}

$(\Rightarrow t \leq r_{k+2})$

Ergebnis: r_{k+2} ist der größte gemeinsamer Teiler von m und n

symbolisch $r_{k+2} = ggT(m,n) = (m,n)$

Jeder gemeinsamer Teiler von m und n ist Teiler von (m,n). $M = \{t \in \mathbb{N} \mid t/m \wedge t/n\} \Rightarrow (m,n) = \max M$

(m,n) ist auch das Maximum von M bezüglich der durch die Teilbarkeit gegebenen Ordnung auf $\mathbb{N}$.

$T_m = \{t \in \mathbb{N} \mid t/m\}; \; T_M \cap T_n = T_{(m,n)}$

$(672, 729)$

$729 = 672 \cdot 1 + 57$

$672 = 57 \cdot 11 + 45$

$57 = 45 \cdot 1 + 12$

$45 = 12 \cdot 3 + 9$

$12 = 9 \cdot 1 + 3$

$9 = 3 \cdot 3$

ggT: $\mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$

Definition: $m, n \in \mathbb{N}$ m ist ein Vielfaches von n, wenn es ein $q \in \mathbb{N}$ gibt mit $m = n \cdot q$

$\Leftrightarrow$ n ist Teiler von m

Satz: Der größte gemeinsamer Teiler von m und n lässt sich als Differenz von Vielfachen von m und n darstellen: $(m,n) = \begin{cases} m \cdot \tilde{m} - n \cdot \tilde{n} \\ n \cdot \tilde{n} - m \cdot \tilde{m} \end{cases}$

Beweis: 1. Fall $m \mid n$, $n = m \cdot q$ $\quad m = n \cdot 1 - m(q-1)$

2. Fall: $m \nmid n$ Induktion nach der Anzahl der Schritte beim euklidischen Algorithmus:

I.A. $n = m \cdot q_1 + r_1$, $r_1 \mid m \Rightarrow r_1 = (m,n) = n \cdot 1 - m q_1$

I.S. $r_{i+2} = (m, r_1) \overset{IV}{\Rightarrow}$

$$\Rightarrow r_{i+2} = \begin{cases} m \cdot \tilde{m} - r_1 \tilde{r} = m\tilde{m} - (n - m q_1)\tilde{r} = m(\tilde{m} + q_1 \tilde{r}) - n\tilde{r} \\ r_1 \tilde{r} - m\tilde{m} = (n - m q_1)\tilde{r} - m\tilde{m} = n\tilde{r} - m(q_1 \tilde{r} + \tilde{m}) \end{cases}$$

Zusatz: Es gilt immer eine Darstellung der Form $(n,m) = n\tilde{n} - m\tilde{m}$

Beweis: Sei $(m,n) = m \cdot \hat{m} - n \cdot \hat{n} \overset{!}{=} n \cdot \tilde{n} - m \cdot \tilde{m}$

$\Leftrightarrow m(\hat{m} + \tilde{m}) = n(\hat{n} + \tilde{n})$

Wähle q so groß, das gilt $mq > \hat{m}$ $\quad mq > \hat{n}$

Setze $\tilde{m} = mq - \hat{m}$ $\quad \tilde{n} = mq - \hat{n}$

$\Rightarrow m(\hat{m} + \tilde{m}) = m \cdot n \cdot q = n(\hat{n} + \tilde{n})$

Definition: $m, n \in \mathbb{N}$ heißen teilerfremd, wenn gilt $(m,n) = 1$.
Dann gibt es $\tilde{m}, \tilde{n}$ mit $m \cdot \tilde{m} - n \cdot \tilde{n} = 1$

Satz: $m, n \in \mathbb{N}$, $m_1 = m : (m,n)$, $n_1 = n : (m,n)$
$\Rightarrow m_1, n_1$ teilerfremd.

Satz: $k \mid m \cdot n$, k, m teilerfremd $\Rightarrow k \mid n$

Beweis: k, m teilerfremd $\Rightarrow$ Wir finden $\tilde{k}, \tilde{m}$ mit $k\tilde{k} - m\tilde{m} = 1$

$\Rightarrow n \cdot k \cdot \tilde{k} - n \cdot m \cdot \tilde{m} = n$
$k \mid n \cdot k \cdot \tilde{k}$ $\quad k \mid m \cdot n \cdot \tilde{m}$
$\Rightarrow k \mid n$