Mathematik-Vormittag 28.10.09

$54 = 15 \cdot 3 + 9$

$15 = 9 \cdot 1 + 6$

$9 = 6 \cdot 1 + \boxed{3} \Rightarrow ggT(54, 15)$

$6 = 3 \cdot 2 + 0$

$3 = 54 \cdot e + 15 \cdot f$

$e, f \in \mathbb{Z}$

$ggT(a,b) = a \cdot e + b \cdot f,$

$e, f \in \mathbb{Z}$

$3 = 9 - 6 \cdot 1 =$

$= 9 - (15 - 9 \cdot 1) \cdot 1 =$

$= 2 \cdot 9 - 15 \cdot 1 =$

$= 2 \cdot (54 - 15 \cdot 3) - 15 \cdot 1 =$

$= 2 \cdot 54 - 7 \cdot 15$

Primzahlen, wir betrachten $\mathbb{N} \setminus \{0\}$

P-Primzahl $:\Leftrightarrow$ ein Teiler sind:

$p > 1$ $\pm 1, \pm p$

→

p Primzahl, $a, b \in \mathbb{N}$

$p \mid a \cdot b \Rightarrow p \mid a \overset{\text{oder}}{\vee} p \mid b$

- Fall $p \mid a$ ✓
- Fall $p \nmid a$, bekannte $\text{ggT}(p, a) = 1$

$\Rightarrow \boxed{1 = p \cdot e + a \cdot f, \; e, f \in \mathbb{Z}}$

$b = \underbrace{p \cdot e \cdot b}_{p \mid \cdot} + \underbrace{a \cdot f \cdot b}_{p \mid \cdot}$

$\Rightarrow p \mid b$

Verallgemeinern:

$p \mid f_1 \cdot (f_2 \cdot \ldots \cdot f_m)$

$\Rightarrow p \mid f_1 \overset{\text{oder}}{\vee} p \mid f_2 \overset{\text{oder}}{\vee} \ldots \vee p \mid f_m$

Satz von eindeutiger Primfaktorzerlegung:

(HS d. Zahlentheorie)

jede natürl. Zahl $a > 1$ lässt sich eindeutig als Produkt von Primfaktoren darstellen.

$$a = p_1 \cdot p_2 \cdots p_r$$

$p_1, \dots, p_r \in \mathbb{P}$ ... Menge der Primzahlen

es gibt Darstellung:

$a > 1$:

- Fall a ist eine Primzahl

  $a \in \mathbb{P}$ ✓

- $a \notin \mathbb{P} \Rightarrow \exists a_1 \in \mathbb{N}, 1 < a_1 < a$:

  ~~$a = a_1$~~ $a_1 \mid a$

  $\Rightarrow a = a_1 \cdot a_2$ $\quad 1 < a_1, a_2 < a$

Argument auf a_1 und a_2 anwenden

$\Rightarrow \dots \Rightarrow$

$$a = p_1 \cdot p_2 \cdots p_r$$

Darstellung ist eindeutig:

angenommen: $a = p_1 \cdot p_2 \cdots p_r$

$= q_1 \cdot q_2 \cdots q_s$

$= p_1$

$\Rightarrow p_1 \mid q_1 \cdot q_2 \cdots q_s$

$\Rightarrow p_1$ teilt mind. einen der Faktoren $q_1, \dots, q_s$

$p_1 \mid q_i$

o.B.d.A (heißt: Umnummerieren in diesem Fall)

$i = 1$

$p_1 \mid q_1$, aber q_1 ist Primzahl

$\Rightarrow p_1 = q_1$

$\Rightarrow p_2 \cdots p_r = q_2 \cdots q_s$

Iterieren $\Rightarrow p_1 = q_1, p_2 = q_2, \dots$

$r < s$: $1 = q_{r+1} \cdot q_{r+2} \cdots$ $\lightning$ Widerspruch

ist Widerspr.

$\Rightarrow$ n ist selbst eine Primzahl, $\lightning$ zur Annahme

$$a = 2^{\nu_2(a)} \cdot 3^{\nu_3(a)} \cdot 5^{\nu_5(a)} \cdot \ldots$$
$$b = 2^{\nu_2(b)} \cdot 3^{\nu_3(b)} \cdot 5^{\nu_5(b)} \cdot \ldots$$
$$ggT(a,b) = 2^{\min(\nu_2(a),\nu_2(b))} \cdot 3^{\min(\nu_3(a),\nu_3(b))} \cdot \ldots$$
$$kgV(a,b) = 2^{\max(\nu_2(a),\nu_2(b))} \cdot 3^{\max(\nu_3(a),\nu_3(b))} \cdot \ldots$$

$$ggT(a,b) \cdot kgV(a,b) = 2^{\min(\nu_2(a),\nu_2(b)) + \max(\nu_2(a),\nu_2(b))} \cdot 3^{\min(\nu_3(a),\nu_3(b)) + \max(\nu_3(a),\nu_3(b))} \cdot \ldots$$
$$= 2^{\nu_2(a)+\nu_2(b)} \cdot 3^{\nu_3(a)+\nu_3(b)} \cdot \ldots$$
$$= 2^{\nu_2(a)} \cdot 3^{\nu_3(a)} \cdot \ldots \cdot 2^{\nu_2(b)} \cdot 3^{\nu_3(b)} \cdot \ldots$$
$$= a \cdot b$$

$$40 = 2 \cdot 2 \cdot 2 \cdot 5 =$$

$$= 2^{3} \cdot 5^{1}$$

$\nu_2(40) = 3$, $\nu_5(40) = 1$

$\nu_p(a) \ldots \quad \nu_3(40) = 0$

$$a = 2^{\nu_2(a)} \cdot 3^{\nu_3(a)} \cdot 5^{\nu_5(a)} \cdot \ldots$$

$$= \prod_{p \in \mathbb{P}} p^{\nu_p(a)}$$

Produkt Primz.

- es gibt unendliche viele Primzahlen

Beweis durch Widerspruch

angenommen: $\mathbb{P} = \{p_1, p_2, \ldots, p_r\}$

betrachte Zahl: $n = p_1 \cdot p_2 \cdot p_3 \cdots p_r + 1$

$\Rightarrow$ $p_i \nmid n$ analog $p_2 \nmid n, \ldots, p_r \nmid n$

weil angenommen $p_1 \mid n \Rightarrow$

$n = p_1 \cdot \tilde{n}$

$p_1 \cdot \tilde{n} = p_1 \cdot p_2 \cdots p_r + 1$

$\Rightarrow 1 = p_1 \cdot (\tilde{n} - p_2 \cdot p_3 \cdots p_r)$

$\Rightarrow p_1 \mid 1$ ↯ Widerspruch das gilt nicht.