Wiederholung:

Der euklidische Algorithmus

Seien $m, n \in \mathbb{Z}^*$, $|m| < |n|$

Wir definieren $r_0 := |n|$

$r_1 := |m|$

und rekursiv $r_{k+1} := r_{k-1} - q_k r_k \in \{0, \dots, r_k - 1\}$ für ein $q_k \in \mathbb{Z}$

Satz 1.5: Die r_k bilden eine monoton fallende Folge in $\mathbb{N}$, und das letzte r_k ungleich 0 ist (m,n).

Beweis: Wenn $r_{k-1}, r_k \in \mathbb{N}$ existieren, dann existieren auch die gewünschten q_k und r_{k+1} (nach Lemma 1.3).

Dass $0 \leq r_{k+1} < r_k$, folgt aus der Definition von r_{k+1} für $k \geq 1$ und aus der Annahme über m, n für $k = 0$.

Der Algorithmus muss also bei 0 terminieren

Es sei r_k der letzte Term ungleich 0.

Wir zeigen, dass $a := (m,n) \mid r_l \quad \forall\, l \leq k$

Denn $a \mid |n| = r_0$

$a \mid |m| = r_1$

und angenommen $a \mid r_{l-2}$ und $a \mid r_{l-1}$

dann gilt $a \mid (r_{l-2} - q_l r_{l-1}) = r_l$

Also mit Induktion gilt $a \mid r_l \quad \forall\, l \leq k$

Insbesondere gilt $a \mid r_k$

Als nächstes zeigen wir, dass $r_k \mid r_\ell \ \forall\, \ell \leq k$

Denn für $\ell = k$ ist das klar

für $\ell = k-1$ gilt $0 = r_{k+1} = r_{k-1} - q_k r_k$

$\Rightarrow r_{k-1} = q_k r_k$

d.h. $r_k \mid r_{k-1}$

und angenommen $r_k \mid r_{\ell+2}$ und $r_k \mid r_{\ell+1}$

dann gilt auch

$r_k \mid r_{\ell+2} - q_{\ell+1} r_{\ell+1} = r_\ell$

Mit Rückwärts-Induktion gilt also $r_k \mid r_\ell \quad \forall\, \ell \leq k$

Insbesondere gilt $r_k \mid m = \pm r_1$ und $r_k \mid n = \pm r_0$

also gilt $r_k \mid a$ (K 1.4 G))

Aber wir haben schon bewiesen, dass $a \mid r_k$

Und da $a, r_k \in \mathbb{N}$, gilt $r_k = a = (m,n)$ □

Beispiel: Sei $m = 10$, $n = -37$

$r_0 = 37$
$r_1 = 10$

$37 = 3 \cdot 10 + 7$ (wie L 1.2)
$q_1 = 3$

$r_2 = 37 - 3 \cdot 10 = 7$

$10 = 1 \cdot 7 + 3$
$q_2 = 1$

$r_3 = 10 - 1 \cdot 7 = 3$

$7 = 2 \cdot 3 + 1$
$q_3 = 2$

$r_4 = 7 - 2 \cdot 3 = 1$

$3 = 3 \cdot 1 + 0$
$q_4 = 3$

$r_5 = 3 - 3 \cdot 1 = 0$

$(10, -37) = r_4 = 1.$

Um die Darstellung $1 = mx + ny$ zu finden:

$$1 = r_4 = r_2 - q_3 r_3$$
$$= 7 - 2 \cdot 3$$

$$r_2 = r_1 - q_2 r_2$$
$$3 = 10 - 1 \cdot 7$$

$$1 = 7 - 2 \cdot (10 - 1 \cdot 7)$$
$$= 3 \cdot 7 - 2 \cdot 10$$

$$r_2 = r_0 - q_1 r_1$$
$$7 = 37 - 3 \cdot 10$$

$$1 = 3 \cdot (37 - 3 \cdot 10) - 2 \cdot 10$$
$$= 3 \cdot 37 - 11 \cdot 10$$
$$= (-3) \cdot (-37) + (-11) \cdot 10$$

$x = -11$
$y = -3$ ist eine ganzzahlige Lösung von $mX + nY = 1$
$10X + (-37)Y = 1$

Kapitel 2: Primzahlen

In diesem Kapitel betrachten wir (hauptsächlich) $\mathbb{N}^+$

Bemerkung: Jede Zahl $n \in \mathbb{N}^+$ hat die Teiler 1 und n.
Diese heissen die trivialen Teiler

Def: Es sei $p \in \mathbb{N}$, $p > 1$. p heisst eine Primzahl
$\Leftrightarrow$ p besitzt nur die trivialen Teiler 1 und p.

Die Menge der Primzahlen in $\mathbb{N}^+$ bezeichnen wir mit $\mathbb{P}$.

Lemma 2.1: $\forall n \in \mathbb{N}^+$, $n > 1$, $\exists p \in \mathbb{P}$ sodass $p \mid n$

Beweis: Sei $T := \{ m \in \mathbb{N} : m \mid n \text{ und } m > 1 \}$ die Menge aller Teiler von n größer als 1.
Es ist $n \in T$, also $T \neq \emptyset$
Sei p also das kleinste Element von T.
Angenommen $p \notin \mathbb{P}$, dann existiert $k \in \mathbb{N}^+$, $k > 1$ und $k \neq p$ sodass $k \mid p$
Aber dann gilt $k < p$ und $k \mid n$ ↯
Also ist $p \in \mathbb{P}$ □

Bemerkung: Hieraus folgt schon die Existenz einer Primfaktorzerlegung
Seine Eindeutigkeit wird in Satz 2.4 bewiesen.

Lemma 2.2 (Lemma von Euklid)
Sei $p \in \mathbb{P}$ und $a, b \in \mathbb{N}^+$.
$p \mid ab \Rightarrow p \mid a$ oder $p \mid b$

Beweis: Wenn $p \mid a$ ist nichts zu beweisen

Also angenommen $p \nmid a$

Dann ist $(p,a) = 1$ $\quad (p,a) \neq p$ und p hat keine anderen Teiler.

Also existieren $x, y \in \mathbb{Z}$ sodass

$$px + ay = 1 \qquad (\S\ 1.3)$$

$$\Rightarrow \quad pxb + ayb = b$$

$p \mid pxb$ und $p \mid y(ab)$

also $p \mid pxb + ayb = b$. $\square$

Satz 2.3 (Satz von Euklid):

Es gibt unendlich viele Primzahlen.

Beweis: Angenommen es gäbe nur endlich viele, $p_1, p_2, \dots, p_n$

Sei $m := p_1 p_2 \cdots p_n + 1$.

Dann existiert ein $p \in \mathbb{P}$ sodass $p \mid m$ $\quad (\angle\ 2.1)$

und $p = p_i$ für ein i

Also $p \mid p_1 p_2 \cdots p_n = m - 1$

Also existieren $k, l \in \mathbb{N}$ sodass $m - 1 = kp$

$$m = lp = kp + 1$$

$$\Rightarrow (l - k)p = 1$$

$$\Rightarrow l - k = p = 1 \quad \lightning \qquad \square$$

Satz 2.4 (Fundamentalsatz der Arithmetik)

Jede Zahl $n \in \mathbb{N}^+$ ist das Produkt von endlich vielen Primzahlen.

Die Darstellung ist bis auf die Reihenfolge eindeutig.

Bemerkung: Die Darstellung heisst die Primfaktorzerlegung

Das leere Produkt (von 0 Primzahlen) ist gleich 1.

Beweis: Wir beweisen als erstes die Existenz der Zerlegung durch Induktion über n.

Für $n=1$ ist die Existenz klar.

Angenommen die Aussage gelt $\forall m \in \mathbb{N}^+$, $m<n$.

Es gibt $p \in \mathbb{P}$ sodass $p \mid n$ (L 2.1)

also $n = mp$

und $m < n$ also hat m eine Primfaktorzerlegung

$$m = \prod_{i=1}^{r} p_i$$

Dann ist $n = p \cdot \prod_{i=1}^{r} p_i$ eine Primfaktorzerlegung von n.

Es gelt also die Existenz für alle $n \in \mathbb{N}^+$.

Eindeutigkeit:

Angenommen es gibt Zahlen sodass die Zerlegung nicht eindeutig ist

Sei n die kleinste solche Zahl, und p der kleinste nicht-triviale Teiler von n.

Dann ist $p \in \mathbb{P}$ und $n = p \cdot m$, mit $m \in \mathbb{N}^+$ und $m<n$

also ist n eindeutig zerlegbar, $m = \prod_{i=1}^{r} p_i$

also ist $n = p \cdot \prod_{i=1}^{r} p_i$ eine Zerlegung

Sei $n = \prod_{i=1}^{s} q_i$ eine weitere Zerlegung.

Dann ist $p \neq q_i$ für $1 \leq j \leq s$

sonst wäre $m = \frac{n}{p} = \prod_{\substack{i=1 \\ i \neq j}}^{s} q_i$ eine weitere Zerlegung von m.

Aber $p \mid n = \prod_{i=1}^{s} q_i$

$\Rightarrow p \mid \prod_{i=1}^{s-1} q_i$ oder $p \mid q_s$ (Lemma von Euklid)

$\Rightarrow p \mid \prod_{i=1}^{s-2} q_i$ oder $p \mid q_{s-1}$ oder $p \mid q_s$ (Lemma von Euklid)

$\vdots$

$\Rightarrow p \mid q_i$ für mindestens ein $j \in \{1, \dots, s\}$

Aber dann hat q_i einen nicht-trivialen Teiler $\lightning$

Also ist die Zerlegung für alle $n \in \mathbb{N}^+$ eindeutig $\square$

Def: Eine <u>Mersennesche Primzahl</u> ist eine Primzahl der Form

$$p = 2^n - 1 \quad , \quad n \in \mathbb{N} \quad n \text{ prim}$$

Eine <u>Fermatsche Primzahl</u> ist eine Primzahl der Form

$$p = 2^n + 1 \quad , \quad n \in \mathbb{N} \quad , \quad n = 2^m \quad , \quad m \in \mathbb{N}$$

Eine <u>vollkommene Zahl</u> ist eine Zahl n sodass

$$\sum_{\substack{d \in \mathbb{N}^+ \\ d \mid n}} d = 2n$$

Bemerkung: (i) $2^n - 1 \in \mathbb{P} \Rightarrow n \in \mathbb{P}$
(ii) $2^n + 1 \in \mathbb{P} \Rightarrow n = 2^m, m \in \mathbb{N}$ } Übungsaufgabe

Warum haben wir vollkommene Zahlen in einem Kapitel über Primzahlen eingeführt?

Proposition 2.5: Eine gerade Zahl $n \in 2\mathbb{N}$ ist vollkommen
$\Leftrightarrow$ n hat die Form $n = 2^m(2^{m+1} - 1)$ $m \in \mathbb{N}$
und 2^{m+1} ist eine Mersennesche Primzahl.

Beweis: Nächstes Mal.