1 Die Menge der natürlichen Zahlen

Für eine Menge M definiere $M^+ = M \cup \{M\}$.

1.1 Die Wohlordnung der natürlichen Zahlen

Für $n, m \in \mathbb{N}$ gilt $n < m$ genau dann, wenn $n \in m$. Wir schreiben $n \leq m$ falls $n < m$ oder $n = m$ gilt. Die Relation $\leq$ ist eine *Wohlordnung:* Für jede Teilmenge T von $\mathbb{N}$ existiert ein *kleinstes Element*. Das heißt für jedes $T \subseteq \mathbb{N}$ gibt es ein Element $x \in T$, so dass es kein $y \in T$ gibt mit $y < x$. Wir bemerken, dass $<$ und $\leq$ binäre Relation auf $\mathbb{N}$ sind, weshalb wir $\leq$ als die Teilmenge von $\mathbb{N} \times \mathbb{N}$ betrachten, die alle geordneten Paare (m, n) enthält mit $n \leq m$.

1.2 Addition und Multiplikation

Die Addition ist eine Funktion $+ := \mathbb{N} \times \mathbb{N} \to \mathbb{N}$(= eine "zweistellige" Funktion auf $\mathbb{N}$) und wird wiefolgt induktiv definiert:

$$n + 0 := n$$
$$n + m^+ := (n + m)^+$$

Auch die Multiplikation $\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ kann mein induktiv definieren:

$$n \cdot 0 := 0$$
$$n \cdot m^+ := n \cdot m + n$$

Und zum Schluss betrachten wir noch die Exponentation $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$ mit Hilfe der Multiplikation:

$$n^0 := 1$$
$$n^{m^+} := n^m n$$

1.3 Teilbarkeit und Primzahlen

Wir definieren auf $\mathbb{N}$ die *Teilbarkeitsrelation:* für $a, b \in \mathbb{N}$ gelte $a \mid b$(sprich a *teilt* b) genau dann, wenn es ein $k \in \mathbb{N}$ gibt mit $a \cdot k = b$. In diesem Fall heißt a *Teiler* von b.

Definition 1 *Eine Zahl $p \in \mathbb{N}$ heißt Primzahl(oder prim), wenn sie größer als 1 ist und nur durch 1 und sich selbst teilbar ist. Ein Primteiler von n ist ein Teiler von n, der prim ist.*

Satz 1 *(Fundamentalsatz der Arithmetik). Jede natürliche Zahl $n > 0$ kann auf genau eine Weise als Produkt*

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$$

geschrieben werden, wobei $k \in \mathbb{N}, p_1 < p_2 < \ldots < p_k$ Primzahlen, und $\alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{N}$ größer als 1 sind.

1.4 Der euklidische Algorithmus

Der euklidische Algorithmus ist ein effizientes Verfahren, um den größten gemeinsamen Teiler zweier Zahlen zu berechen.
Der *größte gemeinsame Teiler* von $a, b \in \mathbb{N}$ ist die größte natürliche Zahl d, die a und b teilt. Wir schreiben $ggT(a, b)$ für diese Zahl d.

Lemma 1 *(Division mit Rest). Seien $a, b \in \mathbb{Z}$ und $b! = 0$. Dann gibt es $q, r \in \mathbb{Z}$ mit $a = qb + r$ und $0 \leq r < |b|$.*

Für die Zahl r aus dem Lemma schreiben wir auch $amodb$; was wir schon unter dem *Rest* aus der schriftlichen Division her kennen. Für $q \in \mathbb{Q}$ schreiben wir $\rfloor q \rfloor$ für die eindeutige größte Zahl $z \in \mathbb{Z}$ die kleiner ist als q. Dann gilt für $a, b \in \mathbb{N}$ und $b! = 0$ dass $a = \rfloor a \setminus b \rfloor + amodb$.

Lemma 2 *Es seien $a, b \in \mathbb{N}$ mit $b > 0$. Dann gilt $ggT(a, b) = ggT(b, amodb)$.*

Dieses Lemma ist die zentrale Beobachtung für die Korrektheit für den euklidischen Algorithmus:
//Eingabe: $m, n \in \mathbb{N}$ mit $m \leq n$
//Ausgabe: $ggT(m, n)$.
Falls $m \mid n$
gebe m aus
ansonsten
gebe $EUKLID(n \mod m, m)$ aus.

1.5 Erweiterter euklidischer Algorithmus

Durch eine kleiner Erweiterung kann der euklidische Algorithmus auch dazu verwendet werden, um für gegeben $m, n \in \mathbb{N}$ die Zahlen $a, b \in \mathbb{Z}$ aus dem Lemma von Bézout zu berechnen.

Lemma 3 *Es seien $m, n \in \mathbb{N}$ nicht beide 0. Dann gibt es ganze Zahlen $a, b \in \mathbb{Z}$ mit $ggT(m, n) = am + bn$.*

Erweiterter Algorithmus:
//Der erweiterte euklidische Algorithmus E-EUKLID(m, n)
//Eingabe: $m, n \in \mathbb{N}$ mit $m \leq n$.
//Ausgabe: $a, b \in \mathbb{Z}$ so dass $ggT(m, n) = am + bn$
Falls $m \mid n$
gebe $(1, 0)$ aus.
ansonsten
Sei (b', a') die Ausgabe von E-EUKLID$(n \mod m, m)$.
Gebe $(a' - b' \rfloor n \setminus m \rfloor, b')$ aus.

Lemma 4 *(Lemma von Euklid). Teilt eine Primzahl das Produkt zweier natürlicher Zahlen, so auch mindestens einen der Faktoren.*