Die Einheitengruppe $U(\mathbb{Z}/n)$.

Ist R ein Ring, so bezeichnet $U(R)$ die *Einheitengruppen* von R, also die Menge der (bezüglich der Multiplikation) invertierbaren Elemente — diese bilden bezüglich der Multiplikation eine Gruppe.

Wir betrachten den Ring $\mathbb{Z}/n$ der Restklassen ganzer Zahlen modulo n (hier ist $n \geq 1$ eine natürliche Zahl). Die Restklasse $\overline{a}$ der ganzen Zahl a mit $1 \leq a \leq n$ ist genau dann im Ring $\mathbb{Z}/n$ invertierbar, wenn $(a, n) = 1$ gilt. Insbesondere gilt:

$$|U(\mathbb{Z}/n)| = \phi(n) \quad \text{(hier ist } \phi \text{ die Euler'sche } \phi\text{-Funktion)}$$

Ist $n = p_1^{e_1} \cdots p_r^{e_r}$ mit paarweise verschiedenen Primzahlen $p_1, \ldots, p_r$, so gilt:

$$\boxed{U(\mathbb{Z}/n) = U(\mathbb{Z}/p_1^{e_1}) \times \cdots \times U(\mathbb{Z}/p_r^{e_r})}$$

(das Gleichheitszeichen ist ein kanonischer Isomorphismus). Dies folgt unmittelbar aus dem chinesischen Restsatz, der ja sogar einen kanonische Isomorphismus von Ringen

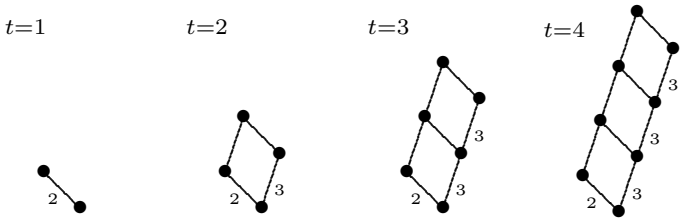
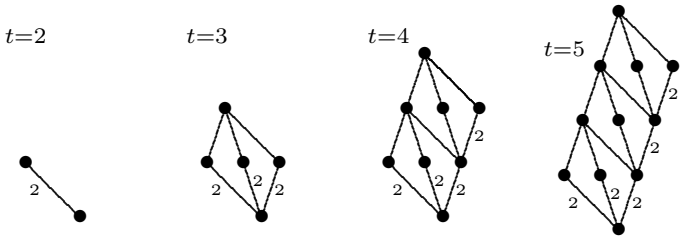
$$\mathbb{Z}/n \longrightarrow \mathbb{Z}/p_1^{e_1} \times \cdots \times \mathbb{Z}/p_r^{e_r},$$

und damit ihrer Einheitengruppen, liefert.

Um die Struktur von $U(\mathbb{Z}/n)$ zu kennen, braucht man also nur den Fall, dass n eine Primzahlpotenz ist, zu studieren.

Satz. *Sei p eine Primzahl und $t \in \mathbb{N}_1$.*
(a) *Ist p ungerade, so ist $U(\mathbb{Z}/p^t)$ zyklisch,* mit Ordnung $\phi(p^t) = p^t - p^{t-1} = (p-1)p^{t-1}$.
(b) Für $p = 2$ gilt: *Es ist $|U(\mathbb{Z}/2)| = 1$. Für $t \geq 2$ ist $U(\mathbb{Z}/2^t)$ das Produkt einer zyklischen Gruppe der Ordnung 2 mit einer zyklischen Gruppe der Ordnung 2^{t-2}.*

$U(\mathbb{Z}/3^t)$



$U(\mathbb{Z}/2^t)$