

Prime Restklassengruppen

$$\begin{aligned} n \in \mathbb{N} \rightarrow \mathbb{Z}_n^\times &= \{\bar{a} \text{ ist invertierbar}\} \\ &= \{\bar{a} \in \mathbb{Z}_n \mid \exists j \in \mathbb{Z}_n : \bar{a}j = 1\} \\ &= \{\bar{a} \in \mathbb{Z}_n \mid \text{ggT}(a, n) = 1\} \end{aligned}$$

$$a, b \text{ sind relativ prim/teilerfremd} \Leftrightarrow \text{ggT}(a, b) = 1$$

$$(\mathbb{Z}_n, +, \cdot) \text{ ist Körper} \Leftrightarrow n \in (\mathbb{P})$$

$$\begin{aligned} \bar{a} \text{ invertierbar} &\Leftrightarrow \exists \bar{b} \in \mathbb{Z}_n && : \bar{a}\bar{b} = \bar{1} \\ &\Leftrightarrow \exists b \in \mathbb{Z} && : (a + n\mathbb{Z})(b + n\mathbb{Z}) = 1 + n\mathbb{Z} \\ &\Leftrightarrow \exists b \in \mathbb{Z} && : n \mid ab - 1 \\ &\Leftrightarrow \exists b \in \mathbb{Z} \exists x \in \mathbb{Z} && : ab - 1 = nx \\ &\Leftrightarrow \exists b \in \mathbb{Z} \exists x \in \mathbb{Z} && : ab - nx = 1 \\ &\Rightarrow && \text{ggT}(a, n) = 1 \end{aligned}$$

Euklidischer Algorithmus

$$a_1 = a, a_2 = b \mid b > 0$$

Sukzessive Division mit Rest:

$$\begin{aligned} a_1 &= q_1 a_2 + a_3, & 0 < a_3 < a_2 \\ a_2 &= q_2 a_3 + a_4, & 0 < a_4 < a_3 \\ \vdots &= \vdots + \vdots & \vdots \\ a_{n-2} &= q_{n-2} a_{n-1} + a_n, & 0 < a_n < a_{n-1} \\ a_{n-1} &= q_{n-1} a_n + 0 & \nwarrow \underline{a_n = \text{ggT}(a_1, a_2)} \end{aligned}$$

$$\exists r, s \in \mathbb{Z} : ra + sb = a_n \quad \Leftarrow \text{erweiterter euklidischer Algorithmus}$$

Eulersche φ -Funktion:

$$\text{Man nennt } \varphi(n) = \#\{a \in \{1, \dots, n\} \mid \text{ggT}(a, n) = 1\}$$

$$\varphi(n) = |\mathbb{Z}_n^\times|$$

$$\varphi(p) = p - 1 \quad \forall p \in \mathbb{P}$$

kleiner Satz von Fermat

$$\text{Es sei } p \in \mathbb{P} \text{ dann gilt: } \forall a \in \mathbb{Z} : a^p \equiv a \pmod{p}$$