Prime Restklassengruppen

$$\begin{aligned} n \in \mathbb{N} \to \mathbb{Z}_n^\times &= \{\overline{a} \text{ ist invertierbar}\} \\ &= \{\overline{a} \in \mathbb{Z}_n \,\big|\, \exists j \in \mathbb{Z}_n : \overline{a}j = 1\} \\ &= \{\overline{a} \in \mathbb{Z}_n \mid ggt(a,n) = 1\} \end{aligned}$$

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

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

$$\begin{array}{lll} \overline{a} \text{ invertierbar} & \Leftrightarrow \exists \overline{b} \in \mathbb{Z}_n & : \overline{a}\overline{b} = \overline{1} \\ & \Leftrightarrow \exists b \in \mathbb{Z} & : (a + n\mathbb{Z})(b + n\mathbb{Z}) = 1 + n\mathbb{Z} \\ & \Leftrightarrow \exists b \in \mathbb{Z} & : n \big| ab - 1 \\ & \Leftrightarrow \exists b \in \mathbb{Z}\ \exists x \in \mathbb{Z} & : ab - 1 = nx \\ & \Leftrightarrow \exists b \in \mathbb{Z}\ \exists x \in \mathbb{Z} & : ab - nx = 1 \\ & \Rightarrow & ggT(a,n) = 1 \end{array}$$

Euklidischer Algorithmus

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

Sukzessive Division mit Rest:

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

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

Erweiterte Euklidischer Algorithmus

Der Erweiterte Euklidischer Algorithmus findet zwei weitere Zahlen $s, t \in R$ die eine Linearkombination bilden, die folgende Gleichung erfüllt:

$$s \cdot a + t \cdot b = \mathrm{ggT}(a, b)$$

Berechnung

Bei dem Erweiterten Euklidischen Algorithmus wird die bisherige Folge r_x um drei weitere (q_x, s_x, t_x) erweitert, welche mit der folgenden Formeln bestimmt werden

$$q_{x+1} := \left\lfloor \frac{r_{x-1}}{r_x} \right\rfloor$$

$$r_{x+1} := \begin{cases} a & \text{wenn } x = 0, \\ b & \text{wenn } x = 1 \\ r_{x-1} - q_x \cdot r_x \end{cases}$$

$$\longrightarrow \quad \begin{aligned} \mathrm{ggT}(a, b) &= r_n \\ &= s_n \cdot a + t_n \cdot b \end{aligned} \quad \text{mit } r_{n+1} = 0$$

$$s_{x+1} := \begin{cases} 1 & \text{wenn } x = 0, \\ 0 & \text{wenn } x = 1 \\ s_{x-1} - q_x \cdot s_x \end{cases}$$

$$t_{x+1} := \begin{cases} 0 & \text{wenn } x = 0, \\ 1 & \text{wenn } x = 1 \\ t_{x-1} - q_x \cdot t_x \end{cases}$$

Eulersche φ-Funktion:

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

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

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

kleiner Satz von Fermat

Es sei $p \in \mathbb{P}$ dann gilt: $\forall a \in \mathbb{Z} : a^p \equiv a (mod\ p)$