4 Zahlentheorie II

4.1 Zahlentheoretische Funktionen

4.1.1 Eulersche φ-Funktion

$$\varphi(n) := |\{a \in [n] \mid \mathrm{ggT}(a,n) = 1\}|.$$

Solche a heißen *prime Restes* mod$m$.

Satz 4.1. $p \in \mathbb{P}, \alpha \geq 1 \Rightarrow$

$$\varphi(p^\alpha) = p^{\alpha-1}(p-1).$$

Beweis.
- p^α Kandidaten für prime Reste.
- Genau $p^{\alpha-1}$ Vielfache von p fallen aus. ($\mathrm{ggT}(a,p) = p$)
- $p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1)$.

□

Satz 4.2. m, n *teilerfremd* $\Rightarrow$

$$\varphi(m)\varphi(n) = \varphi(m \cdot n).$$

4.1.2 Teileranzahlfunktion τ

$$\tau(n) := \{t \in \mathbb{N} \mid t|n\}.$$

Satz 4.3. $n = \prod_{\mathbb{P} \ni p|n} p^{\alpha_p} \in \mathbb{N}, \alpha_p \geq 1$ *eindeutige Primfaktorzerlegung.* $\Rightarrow$

$$\tau(n) = \prod_{\mathbb{P} \ni p|n} (\alpha_p + 1).$$

Beweis. $\left.\begin{matrix} 0 \\ 1 \\ \vdots \\ \alpha_p \end{matrix}\right\}$ α_p+1 Möglichkeiten für Exponenten von p in der Primfaktorzerlegung eines Teilers von n. Kombinatorik $\rightsquigarrow$ Behauptung. □

4.1.3 Teilersummenfunktion σ

$$\sigma(n) := \sum_{\mathbb{N} \ni t|n} t.$$

Satz 4.4. $p \in \mathbb{P}, \alpha \geq 1 \Rightarrow$

$$\sigma(p^\alpha) = \frac{p^\alpha - 1}{p-1}.$$

Beweis. Teilersumme: $\sum_{k=0}^{\alpha} p^k = \frac{p^\alpha - 1}{p-1}$. □

Bemerkung. Auch σ ist multiplikativ.

4.2 Potenzreste

4.2.1 Verhalten von Potenzen von $a \mod m$

Satz 4.5. a, m *teilerfremd. Die Folge* $\left(a^k \mod m\right)_{k \in \mathbb{N}}$ *ist rein periodisch.*

Beweis.
- $l := \min_{k \in \mathbb{N}} \left\{\exists j \in \mathbb{N} : a^{j+k} \equiv a^j \mod m\right\}$ (existiert nach Schubfachprinzip) $\rightsquigarrow$

$$a^j \cdot a^l \equiv a^j \mod m$$
$$a^l \equiv a^0 = 1 \mod m \qquad (a^l, m\text{teilerfremd})$$

Also $(a_k \mod m)_k$ rein periodisch mit Periode l.

□

Definition. *Ordnung von* $a \mod m$:

$$\operatorname{ord}_m(a) := \min_{k \in \mathbb{N}} \left\{ a^k \equiv 1 \mod m \right\}.$$

Satz 4.6.

- $a^j \equiv a^k \mod m \quad \Leftrightarrow \quad j \equiv k \mod \operatorname{ord}_m(a)$.
- $a^k \equiv 1 \mod m \quad \Leftrightarrow \quad \operatorname{ord}_m(a) \mid k$.

4.2.2 Satz von Euler-Fermat

Proposition (Kleiner Fermat)**.**

- $a^p \equiv a \mod p$.
- a, p *teilerfremd* $\rightsquigarrow a^{p-1} \equiv 1 \mod p$.

Satz 4.7 (Euler-Fermat)**.** a, m *teilerfremd* $\Rightarrow$

$$a^{\varphi(m)} = 1 \mod m.$$

4.2.3 Primitivwurzeln

a, m teilerfremd. a heißt *Primitivwurzel* $\mod m :\Leftrightarrow$

$$\operatorname{ord}_m(a) = \varphi(m).$$

d.h. $\left(a^k \mod m\right)_k$ nimmt genau $\varphi(m)$ verschiedene Werte an.

Satz 4.8. $m \geq 2$. $\exists$ *Primitivwurzel* $\mod m \Leftrightarrow \exists p \in \mathbb{P} \setminus \{2\}$: *Eines von*:

1. $m = p^\alpha$
2. $m = 2 \cdot p^\alpha$
3. $m = 2$
4. $m = 4$

Es gibt genau $\varphi(\varphi(m))$ *Primitivwurzeln* $\mod m$.