8.5 Die EULERsche phi-Funktion

Eine wichtige Anwendung des chinesischen Restsatzes ist die folgende; sinnvollerweise wird hier stets $n \geq 2$ vorausgesetzt. Die ganzen Zahlen $\bmod n$ bilden den Ring $\mathbb{Z}/n\mathbb{Z}$. Die *multiplikative Gruppe* $\bmod n$, die (auch in der Kryptologie) oft vorkommt, ist besteht genau aus den invertierbaren Elementen dieses Rings und wird abgekürzt als

$$\mathbb{M}_n := (\mathbb{Z}/n\mathbb{Z})^\times.$$

Ihre Ordnung wird durch die EULERsche φ-Funktion beschrieben:

$$\varphi(n) = \#\mathbb{M}_n = \#\{a \in [0 \cdots n-1] \mid a \text{ teilerfremd zu } n\}.$$

Korollar 1 *Sind m und n teilerfremd, so ist $\varphi(mn) = \varphi(m)\varphi(n)$.*

Beweis. Die Aussage des chinesischen Restsatzes bedeutet gerade, dass der natürliche Ring-Homomorphismus

$$F\colon \mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}, \quad x \mapsto (x \bmod m, x \bmod n),$$

bijektiv, also sogar ein Ring-Isomorphismus ist. Außerdem ist $F(\mathbb{M}_{mn}) = (\mathbb{M}_m \times \mathbb{M}_n)$. Also ist

$$\varphi(mn) = \#\mathbb{M}_{mn} = \#\mathbb{M}_m \cdot \#\mathbb{M}_n = \varphi(m)\varphi(n),$$

wie behauptet. $\diamond$

Ist p prim, so $\varphi(p) = p - 1$, allgemeiner $\varphi(p^e) = p^e - p^{e-1} = p^e(1 - \frac{1}{p})$, wenn $e \geq 1$, denn p^e hat genau die Teiler px mit $1 \leq x \leq p^{e-1}$. Aus Korollar 1 folgt also:

Korollar 2 *Ist $n = p_1^{e_1} \cdots p_r^{e_r}$ die Primfaktorzerlegung (alle $e_i \geq 1$), so*

$$\varphi(n) = n \cdot \prod_{i=1}^{r} (1 - \frac{1}{p_i}).$$