§ 9. Der Satz von Euler/Fermat

(9.1) DEF: Für $n \in \mathbb{N}$ bezeichne

$$\mathcal{R}_n := \{0, 1, 2, \ldots, n-1\}$$

die Menge der nichtnegativen Reste bei Division durch n und

$$\mathcal{R}'_n := \{\, k \mid k \in \mathcal{R}_n\,,\ \mathrm{ggT}(k, n) = 1 \,\}$$

die Menge der zu n teilerfremden Zahlen aus $\mathcal{R}_n$.

Beispiele: $\mathcal{R}_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ $\quad \mathcal{R}'_{10} = \{1, 3, 7, 9\}$

$\mathcal{R}_{11} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ $\quad \mathcal{R}'_{11} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

(9.2) DEF: Die Abbildung $\varphi : \mathbb{N} \longrightarrow \mathbb{N}$ sei definiert durch

$$\varphi(n) := |\mathcal{R}'_n| \quad (n \in \mathbb{N})\,.$$

φ heißt die **Euler'sche Funktion**.

Einige Werte von $\varphi(n)$:

n	1	2	3	4	5	6	10	11
$\varphi(n)$	1	1	2	2	4	2	4	10

(9.3) SATZ: Für eine Primzahl p gilt:

a) $\varphi(p) = p - 1$ $\quad$ **b)** $\varphi(p^k) = p^k - p^{k-1}$ für alle $k \in \mathbb{N}$.

(9.4) SATZ: Für zwei verschiedene Primzahlen p und q gilt

$$\varphi(p \cdot q) = (p-1) \cdot (q-1) = \varphi(p) \cdot \varphi(q)\,.$$

(9.5) BEM: **a)** Man kann allgemein zeigen: Für teilerfremde natürliche Zahlen m und n gilt

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

Man nennt die Abbildung φ daher **multiplikativ**. (9.4) ist ein Spezialfall davon.

b) Damit kann man $\varphi(n)$ für beliebige $n \in \mathbb{N}, n \geq 2$ mit Hilfe der Primfaktorzerlegung von n berechnen.

Beispiel: $72 = 2^3 \cdot 3^2$

$\varphi(72) = \varphi(2^3) \cdot \varphi(3^2) = (2^3 - 2^2) \cdot (3^2 - 3^1) = 4 \cdot 6 = 24$.

Allgemein: Besitzt die natürliche Zahl $n \geq 2$ die Primfaktorzerlegung

$$n = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_r^{k_r}$$

mit paarweise verschiedenen Primzahlen $p_1, p_2, \ldots, p_r$ und Exponenten $k_i \geq 1$, so gilt

$$\begin{aligned} \varphi(n) &= \varphi\left(p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_r^{k_r}\right) \\ &= \varphi\left(p_1^{k_1}\right) \cdot \varphi\left(p_2^{k_2}\right) \cdot \ldots \cdot \varphi\left(p_r^{k_r}\right) \\ &= \left(p_1^{k_1} - p_1^{k_1-1}\right) \cdot \left(p_2^{k_2} - p_2^{k_2-1}\right) \cdot \ldots \cdot \left(p_r^{k_r} - p_r^{k_r-1}\right) \end{aligned}$$

(9.6) SATZ: Seien $n \in \mathbb{N}$ und $\mathcal{R}'_n = \{r_1, r_2, \ldots, r_s\}$ mit $s := \varphi(n)$. Für eine beliebige ganze Zahl $a \in \mathbb{Z}$ mit $\mathbf{ggT}(a, n) = 1$ gilt dann:

a) Es existiert genau ein $t \in \{1, 2, \ldots, s\}$ mit $a \bmod n = r_t$

b) Für $k, l \in \{1, 2, \ldots, s\}$ mit $k \neq l$ ist

$$(a r_k) \bmod n \neq (a r_l) \bmod n$$

c) $\mathcal{R}'_n = \{\, (a r_k) \bmod n \mid k \in \{1, 2, \ldots, s\} \,\}$.

(9.7) SATZ von Euler/Fermat (Euler, 1760)

Für $n \in \mathbb{N}$ und $a \in \mathbb{Z}$ mit $\mathbf{ggT}(a, n) = 1$ gilt:

$$a^{\varphi(n)} \bmod n = 1.$$

(9.8) FOLGERUNG: Kleiner Satz von Fermat (1640)

Für eine Primzahl p und eine zu p teilerfremde ganze Zahl a gilt

$$a^{p-1} \bmod p = 1.$$

Mit dem folgenden Satz, der eine Folgerung aus dem Satz von Euler/Fermat ist, lassen sich Potenzen modulo $\boldsymbol{n}$ leichter berechnen.

(9.9) SATZ: Seien $\boldsymbol{k, n \in \mathbb{N}}$ und $\boldsymbol{a \in \mathbb{Z}}$ mit $\boldsymbol{\mathbf{ggT}(a,n) = 1}$. Ferner sei $\boldsymbol{r = k \bmod \varphi(n)}$. Dann gilt

$$\boldsymbol{a^k \bmod n \;=\; a^r \bmod n\,.}$$

Bew: Es gibt $\boldsymbol{q \in \mathbb{N}_0}$ mit $\boldsymbol{k = q \cdot \varphi(n) + r}$ und $\boldsymbol{0 \le r < \varphi(n)}$.
Auf Grund der Potenzrechenregeln ergibt sich dann

$$(\star) \qquad \boldsymbol{a^k \;=\; a^{q\cdot\varphi(n)+r} \;=\; a^{q\cdot\varphi(n)} \cdot a^r \;=\; \left(a^{\varphi(n)}\right)^q \cdot a^r}$$

Nach (9.7) gilt

$$\boldsymbol{a^{\varphi(n)} \bmod n \;=\; 1}$$

Wir wenden jetzt die Rechenregeln aus der Aufgabe 35 an:

$$\begin{array}{lrcll}
 & \boldsymbol{a^{\varphi(n)} \bmod n} & \boldsymbol{=} & \boldsymbol{1 \bmod n} & \boldsymbol{\mid\hat{}\, q} \\
\boldsymbol{\Longrightarrow} & \boldsymbol{\left(a^{\varphi(n)}\right)^q \bmod n} & \boldsymbol{=} & \boldsymbol{(1^q) \bmod n} & \boldsymbol{\mid \cdot a^r} \\
\boldsymbol{\Longrightarrow} & \boldsymbol{\left(\left(a^{\varphi(n)}\right)^q \cdot a^r\right) \bmod n} & \boldsymbol{=} & \boldsymbol{(1 \cdot a^r) \bmod n} & \\
\boldsymbol{\Longrightarrow} & \boldsymbol{a^k \bmod n} & \boldsymbol{=} & \boldsymbol{a^r \bmod n} & \text{wegen } \boldsymbol{(\star)}
\end{array}$$

Damit ist der Satz bewiesen, und es folgen zwei Beispiele:

Beispiele: **a)** Berechne $\boldsymbol{4^{44} \bmod 7}$

Es ist $\boldsymbol{\mathbf{ggT}(4,7) = 1}$, $\boldsymbol{\varphi(7) = 6}$ und $\boldsymbol{44 \bmod 6 = 2}$. Daher folgt mit (9.9)

$$\boldsymbol{4^{44} \bmod 7 \;=\; 4^2 \bmod 7 \;=\; 16 \bmod 7 \;=\; 2}$$

b) Bestimme die letzten beiden Ziffern von $\boldsymbol{3^{403}}$

Es ist $\boldsymbol{3^{403} \bmod 100}$ zu berechnen (Wieso?)
$\boldsymbol{\mathbf{ggT}(3,100) = 1}$, $\boldsymbol{\varphi(100) = \varphi(2^2 \cdot 5^2) = (2^2 - 2^1) \cdot (5^2 - 5^1) = 2 \cdot 20 = 40}$,
$\boldsymbol{403 \bmod 40 = 3}$. Daher gilt nach (9.9)

$$\boldsymbol{3^{403} \bmod 100 \;=\; 3^3 \bmod 100 \;=\; 27}$$

und die Zahl $\boldsymbol{3^{403}}$ endet mit den beiden Ziffern $\boldsymbol{2, 7}$.