Sätze von Euler und Fermat

Sätze von Euler und Fermat – Eulersche Phifunktion

Wir wollen jetzt Potenzen effizient modulo m berechnen: $a^e \equiv ? \mod m$

ü Berechnen Sie effizient (ohne Taschenrechner):

a) $3^{160} \equiv ? \mod 10 = (3^4)^{80} \equiv 9^{80} \equiv -1^{80} \equiv 1$

b) $3^{161} \equiv ? \mod 9 \equiv 3 \cdot (9)^{80} \equiv 3 \cdot 1^{80} \equiv 3 \cdot 1 \equiv 3$

Idee: Wann gilt $a^e \equiv 1 \mod m$? Dazu braucht man:

Def. Sei $m \in \mathbb{N}$:

$$\varphi(m) := \left| \{ x \in \mathbb{N} \mid 1 \le x \le m \wedge ggT(x,m) = 1 \} \right|$$

= Anzahl der zu m teilerfremden Zahlen zwischen $1, \dots, m$.

heißt **Eulersche Phifunktion**.

ü Bestimmen Sie:

a) $\varphi(6) = 2$, da $x = \underline{1}, 2, 3, 4, \underline{5}, 6$ ($ggT(x,6) = 1$)

b) $\varphi(8) = 4$, da $x = 1; 3; 5; 7$

c) $\varphi(19) = 18$, da $x = 1 - 18$

d) $\boxed{\varphi(p) = p - 1}$, da $x = \underline{1}, \underline{2}, \underline{3}, \dots, \underline{p-1}, p$

(p: Primzahl)

Sätze von Euler und Fermat – Satz von Euler

Mit Hilfe der Eulerschen Phi-Funktion kann man formulieren:

Satz von Euler. Für $ggT(a,m) = 1$: $\boxed{a^{\varphi(m)} \equiv 1 \mod m}$

Beweis. Es gelte $ggT(a;m) = 1$

zu m teilerfremde Zahlen aus $\mathbb{Z}_m$: $k_1; k_2; \dots; k_{\varphi(m)}$

$m = 8 \quad \varphi(8) = 4 \quad 1 \; 3 \; 5 \; 7$

$3 \; 1 \; 7 \; 5$

$ak_1; ak_2; \dots; ak_{\varphi(m)}$

$\Rightarrow ggT(ak_i; m) = 1$

$a \cdot k_i \not\equiv a \cdot k_j \mod m$

$\begin{pmatrix} ak_i \equiv ak_j \mod m \\ k_i \equiv k_j \mod m \end{pmatrix}$ ↯

$k_1 \cdot k_2 \cdot k_3 \cdot \dots \cdot k_{\varphi(m)} = ak_1 \cdot \dots \cdot ak_{\varphi(m)}$

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

Übung Berechnen Sie mit Hilfe von Euler:

a) $7^4 \equiv ? \mod 8 \quad \varphi(8) = 4 \quad 7^4 \equiv 1 \mod 8$

b) $7^{44} \equiv ? \mod 8 \quad (7^4)^{11} \equiv 1^{11} \equiv 1 \mod 8$

c) $7^{45} \equiv ? \mod 8 \equiv 7 \cdot (7^4)^{11} \equiv 7 \cdot 1 \equiv 7 \mod 8$

Sätze von Euler und Fermat – kleiner Satz von Fermat

Als Spezialfall des Satzes von Euler ($m = p$ prim):

kleiner Satz von Fermat. Für $p \nmid a$: $\boxed{a^{p-1} \equiv 1 \mod p}$

Ü Berechnen Sie:

a) $2^{16} \equiv ? \mod 17 \quad = 1$

b) $32^{16} \equiv ? \mod 17 \quad \equiv 1$

c) $32^{33} \equiv ? \mod 17 \equiv 32 \cdot 32^{32} \equiv 32 \cdot 32^{16} \cdot 32^{16} \equiv 32 \cdot 1 \cdot 1 \equiv 32$