Sätze von Euler und Fermat

Sätze von Euler und Fermat – Eulersche Phifunktion

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

ü Berechnen Sie effizient (ohne Taschenrechner):

a) $3^{160} \equiv ?\ \mathrm{mod}\ 10$

b) $3^{161} \equiv ?\ \mathrm{mod}\ 8$

Idee: Wann gilt $a^e \equiv 1\ \mathrm{mod}\ m$? 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) $\varphi(6) =$, da $x = \underline{1}, \cancel{2}, \cancel{3}, \cancel{4}, \underline{5}, \cancel{6}$ ($ggT(x,6) = 1$)

b) $\varphi(8) =$, da $x =$

c) $\varphi(19) =$, da $x =$

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

(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.

ü Berechnen Sie mit Hilfe von Euler:

a) $7^4 \equiv ? \mod 8$

b) $7^{44} \equiv ? \mod 8$

c) $7^{45} \equiv ? \mod 8$

Sätze von Euler und Fermat – kleiner Satz von Fermat

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

kleiner Satz von Fermat. Für $p \nmid a$: $\equiv 1 \mod p$

Ü Berechnen Sie:

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

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

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