

26. Potenzieren modulo n

Wollen ausrechnen:

$$2^{100000} \bmod 100001$$

Schreiben als Summe von Zweierpotenzen:

$$100000 = 2^{2^{16}} + 2^{2^{15}} + 2^{2^{10}} + 2^{2^9} + 2^{2^7} + 2^{2^5}$$

Binärschreibweise:

$$1100001101010000$$

Geschickt klammern:

$$2^{100000} = 2^{2^{16}} \cdot 2^{2^{15}} \cdot 2^{2^{10}} \cdot 2^{2^9} \cdot 2^{2^7} \cdot 2^{2^5}$$

TRICK: Zwischenergebnis modulo 100001 (Homomorphieregel)