DSA Primzahlen

q mit 224 bzw 256 Bits

p mit 2048 Bits

q teilt $p-1 \Rightarrow p = q \cdot t + 1$

für einen Teiler t

Primzahltest: Miller-Rabin

vereinfachter Test

$$a^{\frac{p-1}{2}} \equiv \pm 1 \bmod p$$

ja → p wahrsch. Primzahl

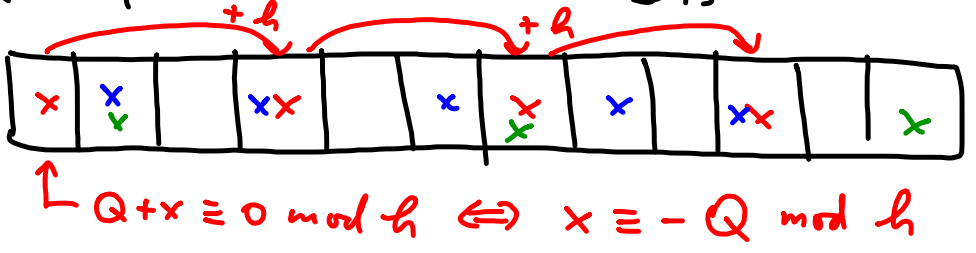
nein → p keine Primzahl

Beschleunigung:

weniger Primzahltests, vorher aussieben

q wählen

Q Zufallszahl mit 224 Bits



$Q + x \equiv 0 \bmod h \Leftrightarrow x \equiv -Q \bmod h$

Algorithmus:

Initialisieren Siebarray  mit false

for h in $\{2, 3, 5, \ldots, H\}$

$x \equiv -Q \bmod h$

Sieb ab $Q + x$ im Abstand h ($\rightarrow$ true)

Primzahltest für alle Einträge, die noch false sind