Erzeuger finden

① $p = 11, \quad p - 1 = 2 \cdot 5$

$g = 2$: ✓

$$2^{\frac{11-1}{2}} \equiv 2^{5} \equiv 32 \equiv 10 \bmod 11 \quad \neq 1$$

$$2^{\frac{11-1}{5}} \equiv 2^{2} \equiv 4 \bmod 11 \quad \neq 1 \quad ✓$$

$g = 3$: kein Erzeuger

$$3^{\frac{11-1}{2}} \equiv 3^{5} \equiv 3^{3} \cdot 3^{2} \equiv 5 \cdot 9 \equiv 45 \equiv 1 \bmod 11$$

② $p = 101$, $p - 1 = 2^2 \cdot 5^2$

$g = 2$: $g^{\frac{101-1}{2}} \equiv g^{50} \equiv 100 \mod 101$

$g^{\frac{101-1}{5}} \equiv g^{20} \equiv 95 \mod 101$. ✓

③ $p = 997$, $p - 1 = 2^2 \cdot 3 \cdot 83$

$\rightsquigarrow g = 7$

④ $p = 65521$ $\quad p-1 = 2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13$

$\rightsquigarrow g = 29$

Anzahl Erzeuger

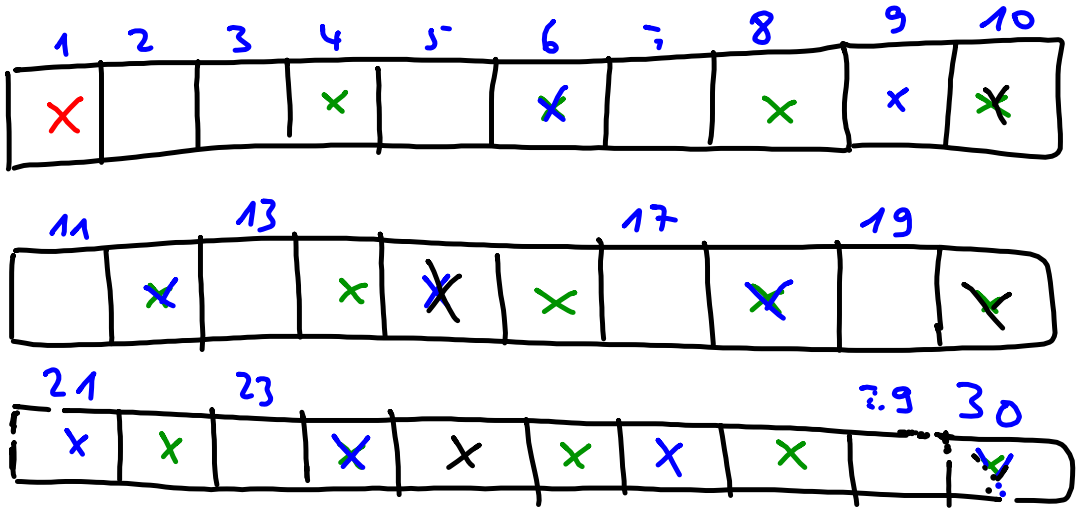
$$\varphi(p-1) = \varphi(2^4) \cdot \varphi(3^2) \cdot \varphi(5) \cdot \varphi(7) \cdot \varphi(13)$$

$$= (2^4 - 2^3) \cdot (3^2 - 3) \cdot 4 \cdot 6 \cdot 12$$

$$= 8 \cdot 6 \cdot 24 \cdot 12 = 96 \cdot 144 = 13824$$

Primzahlen finden

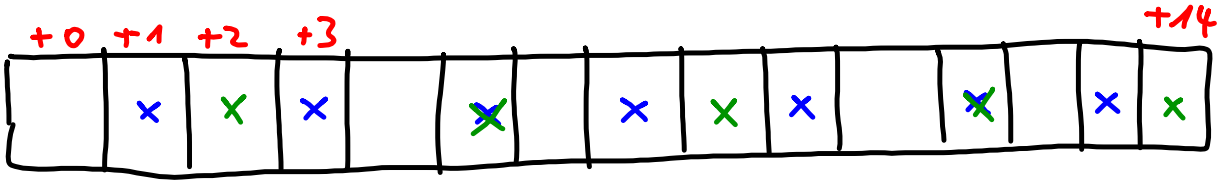
Sieb des Eratosthenes für "kleine" Primzahlen



große Primzahlen

- Probedivision mit kleinen Primzahlen
- Primzahltest (→ Miller-Rabin)

Sieb



n_0 Minimum für gesuchte Primzahl

Das Sieb testet Zahlen der Form

$$n_0 + i$$

auf kleine Teiler t (s.o. Eratosthenes)

Wo gilt $t \mid (n_0 + i)$?

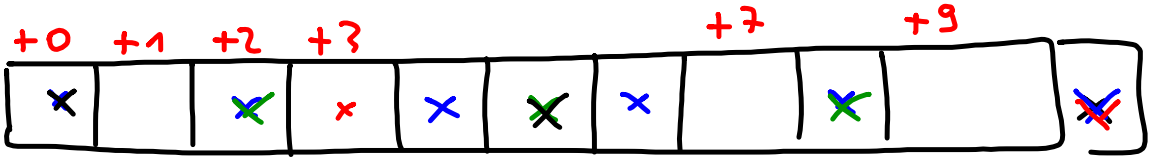
$$n_0 + i \equiv 0 \mod t$$

$$\Leftrightarrow \quad i \equiv -n_0 \mod t$$

Beispiel:

wir suchen die erste Primzahl > 10.000

$n_0 = 10.000$



$t = 2 \Rightarrow \quad i \equiv -n_0 \equiv -10000 \equiv 0 \bmod 2$ ×

$t = 3 \Rightarrow \quad i \equiv -n_0 \equiv -10000 \equiv 2 \bmod 3$ ×

Primzahltests

nutzen als Grundidee

$A \Rightarrow B$

$\overline{A} \Leftarrow \overline{B}$

p Primzahl $\Rightarrow$ $a^{p-1} \equiv 1 \bmod p$

$a \in \mathbb{N}$, $ggT(a,p)=1$

kleiner Satz des Fermat

Beispiele:

① $p = 11$, $a = 2$ $\Rightarrow$ $a^{11-1} \equiv 2^{10} \equiv 2^5 \cdot 2^5$

$\equiv 10 \cdot 10 \equiv 1 \bmod 11$ ✓

② $n = 143$, $a = 2$ — & IP

$A \Rightarrow B$

$a^{143-1} \equiv 2^{142} \equiv 114 \bmod 143$

$\not\equiv 1$

" $\overline{B} \Rightarrow \overline{A}$ "

Pragmatischer Ansatz der Kryptographie:

- $a^{p-1} \equiv 1 \mod p$ für viele a's

Verschärfung von = Miller-Rabin-Primzahltest

- wenn immer $\equiv 1$, dann verkünde "p Primzahl"

Schnelle Exponentiation

$a^x \mod p$ effizient berechnen

$$a^{16} \equiv \left(\left(\left(a^2\right)^2\right)^2\right)^2 \mod p$$

$$a^{21} \equiv \left(\left(\left(a^2\right)^2\right)^2\right)^2 \cdot \left(a^2\right)^2 \cdot a$$

$21 = 16 + 4 + 1$

Laufzeit:

$a^x \bmod p$

Anzahl Quadrierungen: Bitlänge von x

" Multiplikationen: —— " ——

$2 \cdot \lceil \log_2(x) \rceil$

$\bmod^*$: $O(\log^2(p))$