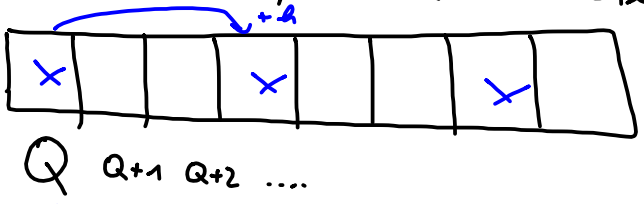
DSA Parameter

q mit 224 Bits

↳ Siebverfahren, kleine Primzahlen h



Startwert für das Sieb mit h: $x \equiv -Q \bmod h$ — $Q + x \equiv 0 \bmod h$

Kandidaten $Q+x$, die nach dem Sieb übrig bleiben, werden mit Primzahltest untersucht, $q = Q + x$

$$a^{\frac{q-1}{2}} \equiv \pm 1 \bmod q \qquad a \in \{2, 3, 5\}$$

Zweite Primzahl finden

p mit $p-1$ durch q teilbar, $p - 1 = t \cdot q$

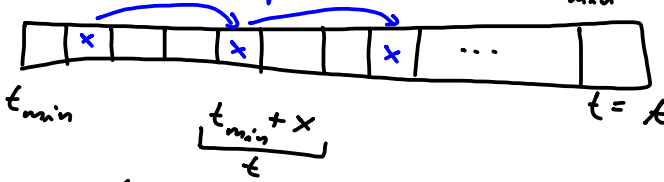
auch hier Siebverfahren möglich, für welche t ist $p = q \cdot t + 1$ eine Primzahl?

Für kleine Primzahlen h sieben wir den Ausdruck $qt + 1$.

Startwert $qt + 1 \equiv 0 \bmod h$

$$\Rightarrow t \equiv -\frac{1}{q} \bmod h$$

$t_{min} = 2^{1824}$, besser: t_{min} Zufallszahl mit 1824 Bits



$$t_{min} + x \equiv -\frac{1}{q} \bmod h$$

$$\Rightarrow x \equiv -\frac{1}{q} - t_{min} \bmod h$$

$$\frac{1}{q} \equiv q^{h-2} \bmod h$$

g wählen

Ziel: $g^q \equiv 1 \mod p$

Algorithmus:

Zufallszahl $\tilde{g}$, $2 \leq \tilde{g} \leq p-2$

teste $\tilde{g}^{\frac{p-1}{q}} \equiv 1 \mod p$

falls ja → Zufallszahl

falls nein, setze $g \equiv \tilde{g}^{\frac{p-1}{q}} \mod p$

Zusammenfassung:

1. q wählen, Q mit 224 Bits, Siebverfahren
2. p wählen, $p = q \cdot t + 1$, t_{min} mit 1824 Bits, Sieb
3. g wählen,
$$g \equiv \tilde{g}^{\frac{p-1}{q}} \mod p$$
4. x wählen geheim
5. $y \equiv g^x \mod p$
6. veröffentliche den DSA public key
$$(p, q, g, y)$$