$n := 7$ <- Antal bits

$r := 2^n = 128$

$m := 21$ <- Montgomery modulo værdi

$a := 19$ <- Selv valgt værdi -> $b := 11$

$A := \mathrm{mod}(a \cdot r, m) = 17$ <- a i montgomery residue

Forventet resultat

$\mathrm{mod}(a \cdot b, m) = 20$

$\gcd(r, m) = 1$

Betingelse for "r" og "m". gcd af r og m SKAL være 1

$$
b := \left|\begin{array}{l}
Bold \leftarrow b \\
\text{for } i \in 0..n \\
\quad \left|\begin{array}{l}
Quotient \leftarrow \mathrm{floor}\left(\frac{Bold}{2}\right) \\
Binary_i \leftarrow \mathrm{ceil}\left(\frac{Bold}{2}\right) - \mathrm{floor}\left(\frac{Bold}{2}\right) \\
\text{if } b = 0 \\
\quad \left|\begin{array}{l}
Binary_i = 0 \\
\text{break}
\end{array}\right. \\
Bold \leftarrow Quotient
\end{array}\right. \\
\text{return } Binary
\end{array}\right.
\qquad
b = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}
$$

Selv valgt værdi i binær-tal

Algoritme for decimal -> bit

$$
S := \left|\begin{array}{l}
S_0 \leftarrow 0 \\
\text{for } i \in 0..n \\
\quad \left|\begin{array}{l}
q_i \leftarrow \mathrm{mod}(S_i, 2) \\
S_{i+1} \leftarrow \mathrm{floor}\left(\frac{S_i + q_i m}{2}\right) + b_i A
\end{array}\right. \\
\text{return } S
\end{array}\right.
= \begin{pmatrix} 0 \\ 17 \\ 36 \\ 18 \\ 26 \\ 13 \\ 17 \\ 19 \\ 20 \end{pmatrix}
$$

Resultat af hvert step i algoritmen.

Algoritme MM skrevet pænt og neat

$$
\mathrm{mod}(S \cdot r, m) = \begin{pmatrix} 0 \\ 13 \\ 9 \\ 15 \\ 10 \\ 5 \\ 13 \\ 17 \\ 19 \end{pmatrix}
$$

Svar i M-res

$i = 0$ <- Første step af algoritmen.

$S_{00} := 0$

$q_0 := \mathrm{mod}(S_{00}, 2) = 0$

$$S_0 := \mathrm{floor}\left(\frac{S_{00} - q_0}{2}\right) + q_0 \cdot \left(\mathrm{floor}\left(\frac{m+1}{2}\right)\right) + b_0 A = 17$$

$i = 1$ <- step 2 af algoritmen

$q_1 := \mathrm{mod}(S_0, 2) = 1$

$$S_1 := \mathrm{floor}\left(\frac{S_0 - q_1}{2}\right) + q_1 \cdot \left(\mathrm{floor}\left(\frac{m+1}{2}\right)\right) + b_1 A = 36$$

$i = 2$ <- step 3 af algoritmen

$q_2 := \mathrm{mod}(S_1, 2) = 0$

$$S_2 := \mathrm{floor}\left(\frac{S_1 - q_2}{2}\right) + q_2 \cdot \left(\mathrm{floor}\left(\frac{m+1}{2}\right)\right) + b_2 A = 18$$

$i = 3$ <- etc.

$q_3 := \mathrm{mod}(S_2, 2) = 0$

$$S_3 := \mathrm{floor}\left(\frac{S_2 - q_3}{2}\right) + q_3 \cdot \left(\mathrm{floor}\left(\frac{m+1}{2}\right)\right) + b_3 A = 26$$

$i = 4$

$q_4 := \mathrm{mod}(S_3, 2) = 0$

$$S_4 := \mathrm{floor}\left(\frac{S_3 - q_4}{2}\right) + q_4 \cdot \left(\mathrm{floor}\left(\frac{m+1}{2}\right)\right) + b_4 A = 13$$

$i = 5$

$q_5 := \mathrm{mod}(S_4, 2) = 1$

$$S_5 := \mathrm{floor}\left(\frac{S_4 - q_5}{2}\right) + q_5 \cdot \left(\mathrm{floor}\left(\frac{m+1}{2}\right)\right) + b_5 A = 17$$

$i = 6$

$q_6 := \mathrm{mod}(S_5, 2) = 1$

$$S_6 := \mathrm{floor}\left(\frac{S_5 - q_6}{2}\right) + q_6 \cdot \left(\mathrm{floor}\left(\frac{m+1}{2}\right)\right) + b_6 A = 19$$

$i = 7$ RESULTAT FOR $n = 7$

$$q_7 := \mathrm{mod}(S_6, 2) = 1$$

$$S_7 := \mathrm{floor}\left(\frac{S_6 - q_7}{2}\right) + q_7 \cdot \left(\mathrm{floor}\left(\frac{m+1}{2}\right)\right) + b_7 A = 20$$

$i = 8$ RESULTAT FOR $n = 8$

$$q_8 := \mathrm{mod}(S_7, 2) = 0$$

$$S_8 := \mathrm{floor}\left(\frac{S_7 - q_8}{2}\right) + q_8 \cdot \left(\mathrm{floor}\left(\frac{m+1}{2}\right)\right) + b_7 A = 10$$

Forventet resultat.
OBS giver ikke altid rigtigt svar

$x := a$ <- Selv valgt værdi -> $e := 14$

$$\mathrm{mod}\left(x^{e}, m\right) = 0$$

$y_{00} := 1$ <- y skal starte med at være 1

$$x^{e} = 799006685782884300$$

Eksponent.
Bare for sjov

$z_{00} := x$ <- $z = x$ i algoritme ME

$$e := \left|\begin{array}{l} \mathrm{Bold} \leftarrow e \\ \text{for } i \in 0..n \\ \quad \left|\begin{array}{l} \mathrm{Quotient} \leftarrow \mathrm{floor}\left(\frac{\mathrm{Bold}}{2}\right) \\ \mathrm{Binary}_i \leftarrow \mathrm{ceil}\left(\frac{\mathrm{Bold}}{2}\right) - \mathrm{floor}\left(\frac{\mathrm{Bold}}{2}\right) \\ \text{if } b = 0 \\ \quad \left|\begin{array}{l} \mathrm{Binary}_i = 0 \\ \text{break} \end{array}\right. \\ \mathrm{Bold} \leftarrow \mathrm{Quotient} \end{array}\right. \\ \text{return } \mathrm{Binary} \end{array}\right.$$

$$e = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

Eksponent i binær-tal

Algoritme for decimal -> bit

$$y := \left|\begin{array}{l} y_0 \leftarrow y_{00} \\ z_0 \leftarrow z_{00} \\ \text{for } i \in 0..n-1 \\ \quad \left|\begin{array}{l} z_{i+1} \leftarrow \mathrm{mod}\left(z_i \cdot z_i, m\right) \\ y_{i+1} \leftarrow \left|\begin{array}{ll} \mathrm{mod}\left(y_i \cdot z_i, m\right) & \text{if } e_i = 1 \\ y_i & \text{otherwise} \end{array}\right. \end{array}\right. \\ \text{return } y \end{array}\right. = \begin{pmatrix} 1 \\ 1 \\ 4 \\ 1 \\ 4 \\ 4 \\ 4 \\ 4 \end{pmatrix}$$

Algoritme ME skrevet pænt og neat

$$\mathrm{mod}(y \cdot r, m) = \begin{pmatrix} 2 \\ 2 \\ 8 \\ 2 \\ 8 \\ 8 \\ 8 \\ 8 \end{pmatrix}$$ Svar i M-res

$i := 0 .. n - 1$

$y_0 := y_{00} = 1 \qquad z_0 := z_{00} = 19$

$z_{i+1} := \mathrm{mod}\left(z_i \cdot z_i, m\right)$

$$y_{i+1} := \begin{cases} \mathrm{mod}\left(y_i \cdot z_i, m\right) & \text{if } e_i = 1 \\ y_i & \text{otherwise} \end{cases}$$

$$y = \begin{pmatrix} 1 \\ 1 \\ 4 \\ 1 \\ 4 \\ 4 \\ 4 \\ 4 \end{pmatrix} \qquad z = \begin{pmatrix} 19 \\ 4 \\ 16 \\ 4 \\ 16 \\ 4 \\ 16 \\ 4 \end{pmatrix}$$

Algoritmen skrevet nogenlunde pænt.
Men her får vi også z-værdien

**for** $i$ **=** $0$ **to** $n - 1 = 6$

**do**

$i \mathbf{=} 0$

$e_{0} = 0$

$$y_0 := \begin{cases} \operatorname{mod}(y_{00} \cdot z_{00}, m) & \text{if } e_{0} \mathbf{=} 1 \\ y_{00} & \text{otherwise} \end{cases} = \blacksquare$$

$z_0 := \operatorname{mod}(z_{00} \cdot z_{00}, m) = 4$

$i \mathbf{=} 1$

$e_{1} = 1$

$$y_1 := \begin{cases} \operatorname{mod}(y_0 \cdot z_0, m) & \text{if } e_{1} \mathbf{=} 1 \\ y_0 & \text{otherwise} \end{cases} = \blacksquare$$

$z_1 := \operatorname{mod}(z_0 \cdot z_0, m) = 16$

$i \mathbf{=} 2$

$e_{2} = 1$

$$y_2 := \begin{cases} \operatorname{mod}(y_1 \cdot z_1, m) & \text{if } e_{2} \mathbf{=} 1 \\ y_1 & \text{otherwise} \end{cases} = \blacksquare$$

$z_2 := \operatorname{mod}(z_1 \cdot z_1, m) = 4$

$i \mathbf{=} 3$

$e_{3} = 1$

$$y_3 := \begin{cases} \operatorname{mod}(y_2 \cdot z_2, m) & \text{if } e_{3} \mathbf{=} 1 \\ y_2 & \text{otherwise} \end{cases} \rightarrow$$

$z_3 := \operatorname{mod}(z_2 \cdot z_2, m) = 16$

$i \mathbf{=} 4$

$e_{4} = 0$

$$y_4 := \begin{cases} \operatorname{mod}(y_3 \cdot z_3, m) & \text{if } e_{4} \mathbf{=} 1 \\ y_3 & \text{otherwise} \end{cases} = \blacksquare$$

$z_4 := \operatorname{mod}(z_3 \cdot z_3, m) = 4$

$i = 5$

$e_5 = 0$

$$y_5 := \begin{cases} \mathrm{mod}(y_4 \cdot z_4, m) & \text{if } e_5 = 1 \\ y_4 & \text{otherwise} \end{cases} = \blacksquare$$

$z_5 := \mathrm{mod}(z_4 \cdot z_4, m) = 16$

$i = 6$ FOR $n = 7$

$e_6 = 0$

$$y_6 := \begin{cases} \mathrm{mod}(y_5 \cdot z_5, m) & \text{if } e_6 = 1 \\ y_5 & \text{otherwise} \end{cases} = \blacksquare$$

$z_6 := \mathrm{mod}(z_5 \cdot z_5, m) = 4$

$i = 7$ FOR $n = 8$

$e_7 = 0$

$$y_7 := \begin{cases} \mathrm{mod}(y_6 \cdot z_6, m) & \text{if } e_7 = 1 \\ y_6 & \text{otherwise} \end{cases} = \blacksquare$$

$z_7 := \mathrm{mod}(z_6 \cdot z_6, m) = 16$