$n := 16$ <- Antal bits

$r := 2^n = 6.554 \times 10^4$

$m := 21$ <- Montgomery værdi

Forventet resultat

$a := 18$ <- Selv valgt værdi -> $b := 12$

$\mathrm{mod}(a \cdot b, m) = 6$

$A := \mathrm{mod}(a \cdot r, m) = 15$ <- a i montgomery residue

$\gcd(r, m) = 1$

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

```
b :=  | Bold ← b
      | for i ∈ 0 .. n
      |   | Quotient ← floor(Bold/2)
      |   | Binary_i ← ceil(Bold/2) − floor(Bold/2)
      |   | if b = 0
      |   |   | Binary_i = 0
      |   |   | break
      |   | Bold ← Quotient
      | return Binary
```

Algoritme for decimal -> bit

$b =$

	0
0	0
1	0
2	1
3	1
4	0
5	0
6	0
7	0
8	0
9	0
10	0
11	0
12	0
13	0
14	0
15	...

Selv valgt værdi i binær-tal

$i = 0$ <- Første step af algoritmen.

$S_{00} := 0$

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

$$S_0 := \mathrm{floor}\left(\frac{S_{00} - q_0}{2}\right) + q_0 \cdot \left(\mathrm{floor}\left(\frac{m+1}{2}\right)\right) + b_0 A = 0$$

$i = 1$ <- step 2 af algoritmen

$q_1 := \mathrm{mod}(S_0, 2) = 0$

$$S_1 := \mathrm{floor}\left(\frac{S_0 - q_1}{2}\right) + q_1 \cdot \left(\mathrm{floor}\left(\frac{m+1}{2}\right)\right) + b_1 A = 0$$

$i = 2$ <- step 3 af algoritmen

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

$S_2 := \mathrm{floor}\left(\frac{S_1 - q_2}{2}\right) + q_2 \cdot \left(\mathrm{floor}\left(\frac{m+1}{2}\right)\right) + b_2 A = 15$

$i = 3$ <- etc.

$q_3 := \mathrm{mod}(S_2, 2) = 1$

$S_3 := \mathrm{floor}\left(\frac{S_2 - q_3}{2}\right) + q_3 \cdot \left(\mathrm{floor}\left(\frac{m+1}{2}\right)\right) + b_3 A = 33$

$i = 4$

$q_4 := \mathrm{mod}(S_3, 2) = 1$

$S_4 := \mathrm{floor}\left(\frac{S_3 - q_4}{2}\right) + q_4 \cdot \left(\mathrm{floor}\left(\frac{m+1}{2}\right)\right) + b_4 A = 27$

$i = 5$

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

$S_5 := \mathrm{floor}\left(\frac{S_4 - q_5}{2}\right) + q_5 \cdot \left(\mathrm{floor}\left(\frac{m+1}{2}\right)\right) + b_5 A = 24$

$i = 6$

$q_6 := \mathrm{mod}(S_5, 2) = 0$

$S_6 := \mathrm{floor}\left(\frac{S_5 - q_6}{2}\right) + q_6 \cdot \left(\mathrm{floor}\left(\frac{m+1}{2}\right)\right) + b_6 A = 12$

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

$q_7 := \mathrm{mod}(S_6, 2) = 0$

$S_7 := \mathrm{floor}\left(\frac{S_6 - q_7}{2}\right) + q_7 \cdot \left(\mathrm{floor}\left(\frac{m+1}{2}\right)\right) + b_7 A = 6$

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

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

$S_8 := \mathrm{floor}\left(\frac{S_7 - q_8}{2}\right) + q_8 \cdot \left(\mathrm{floor}\left(\frac{m+1}{2}\right)\right) + b_7 A = 3$

$$
\begin{array}{l}
S_0 \leftarrow 0 \\
\text{for } i \in 0 .. n \\
\quad \left| \begin{array}{l} q_i \leftarrow \mathrm{mod}\left(S_i, 2\right) \\ S_{i+1} \leftarrow \mathrm{floor}\left(\dfrac{S_i + q_i m}{2}\right) + b_i A \end{array} \right. \\
\text{return } S
\end{array}
=
$$

Algoritme MM skrevet pænt og neat

	0
0	0
1	0
2	0
3	15
4	33
5	27
6	24
7	12
8	6
9	3
10	12
11	6
12	3
13	12
14	6
15	...

Resultat af hvert step i algoritmen.

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

$x^{e} = 37481336758208105$

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

Eksponent.
Bare for sjov

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

e =

	0
0	0
1	1
2	1
3	1
4	0
5	0
6	0
7	0
8	0
9	0
10	0
11	0
12	0
13	0
14	0
15	...

Eksponent i binær-tal

Algoritme for decimal -> bit

for $i = 0$ **to** $n - 1 = 15$
do

$i = 0$

$e_0 = 0$

$$y_0 := \left| \begin{array}{ll} \mathrm{mod}\left(y_{00} \cdot z_{00}, m\right) & \text{if } e_0 = 1 \\ y_{00} & \text{otherwise} \end{array} \right. = 1$$

$z_0 := \mathrm{mod}\left(z_{00} \cdot z_{00}, m\right) = 9$

$i = 1$

$e_1 = 1$

$$y_1 := \left| \begin{array}{ll} \mathrm{mod}\left(y_0 \cdot z_0, m\right) & \text{if } e_1 = 1 \\ y_0 & \text{otherwise} \end{array} \right. = 9$$

$z_1 := \mathrm{mod}\left(z_0 \cdot z_0, m\right) = 18$

$i = 2$

$e_2 = 1$

$$y_2 := \begin{cases} \mathrm{mod}(y_1 \cdot z_1, m) & \text{if } e_2 = 1 \\ y_1 & \text{otherwise} \end{cases} = 15$$

$z_2 := \mathrm{mod}(z_1 \cdot z_1, m) = 9$

$i = 3$

$e_3 = 1$

$$y_3 := \begin{cases} \mathrm{mod}(y_2 \cdot z_2, m) & \text{if } e_3 = 1 \\ y_2 & \text{otherwise} \end{cases} \to 9$$

$z_3 := \mathrm{mod}(z_2 \cdot z_2, m) = 18$

$i = 4$

$e_4 = 0$

$$y_4 := \begin{cases} \mathrm{mod}(y_3 \cdot z_3, m) & \text{if } e_4 = 1 \\ y_3 & \text{otherwise} \end{cases} = 9$$

$z_4 := \mathrm{mod}(z_3 \cdot z_3, m) = 9$

$i = 5$

$e_5 = 0$

$$y_5 := \begin{cases} \mathrm{mod}(y_4 \cdot z_4, m) & \text{if } e_5 = 1 \\ y_4 & \text{otherwise} \end{cases} = 9$$

$z_5 := \mathrm{mod}(z_4 \cdot z_4, m) = 18$

$i = 6$ FOR $n = 7$

$e_6 = 0$

$$y_6 := \begin{cases} \mathrm{mod}(y_5 \cdot z_5, m) & \text{if } e_6 = 1 \\ y_5 & \text{otherwise} \end{cases} = 9$$

$z_6 := \mathrm{mod}(z_5 \cdot z_5, m) = 9$

$i = 7$ FOR $n = 8$

$e_7 = 0$

$$y_7 := \begin{cases} \mathrm{mod}(y_6 \cdot z_6, m) & \text{if } e_7 = 1 \\ y_6 & \text{otherwise} \end{cases} = 9$$

$z_7 := \mathrm{mod}(z_6 \cdot z_6, m) = 18$

0

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

	0
0	1
1	1
2	9
3	15
4	9
5	9
6	9
7	9
8	9
9	9
10	9
11	9
12	9
13	9
14	9
15	...

Algoritme ME skrevet pænt og neat

$i := 0 .. n - 1$

$y_0 := y00 = 1$ $\quad$ $z_0 := z00 = 18$

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

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

$y =$

	0
0	1
1	1
2	9
3	15
4	9
5	9
6	9
7	9
8	9
9	9
10	9
11	9
12	9
13	9
14	9
15	...

$z =$

	0
0	18
1	9
2	18
3	9
4	18
5	9
6	18
7	9
8	18
9	9
10	18
11	9
12	18
13	9
14	18
15	...

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