$n := 16$ <- Antal bits

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

$m := 21$ <- Montgomery værdi

Forventet resultat V

$a := 18$ <- 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

```
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

Selv valgt værdi i binær-

12	0
13	0
14	0
15	...

$i = 0$ <- 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 $n = 8$

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

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

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

Algoritme MM skrevet pænt og neat

	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	3
16	12
17	...

Resultat af hvert step i algoritme

Forventet resultat.
OBS giver ikke altid rigtigt sva

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

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

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

$x^{e} = 3748133675820810$

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

Eksponent. Bare for sjc

1

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

tal

Algoritme for decimal -> bit

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

Eksponent i binær-ta

14	0
15	...

for i **=** 0 **to** n − 1 = 15

do

$i = 0$

$e_0 = 0$

$$y_0 := \begin{cases} \mathrm{mod}(y_{00} \cdot z_{00}, m) & \text{if } e_0 = 1 \\ y_{00} & \text{otherwise} \end{cases} = 1$$

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

$i = 1$

$e_1 = 1$

$$y_1 := \begin{cases} \mathrm{mod}(y_0 \cdot z_0, m) & \text{if } e_1 = 1 \\ y_0 & \text{otherwise} \end{cases} = 9$$

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

$i = 2$

$e_2 = 1$

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

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

$i = 3$

$e_3 = 1$

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

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

$i = 4$

$e_4 = 0$

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

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

$i = 5$

$e_5 = 0$

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

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

$i = 6$ 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 $n = 8$

$e_7 = 0$

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

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

n.

r

50

ov

al

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

	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

$i := 0..n-1$

$y_0 := y_{00} = 1$ $\quad z_0 :=$

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

$$y_{i+1} := \left|\begin{array}{ll} \operatorname{mod}(y_i \cdot z_i, m) & \text{i} \\ y_i & \text{otherwise} \end{array}\right.$$

	0
0	1

0

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

y =

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 =

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