$\mathbb{Z}_2[x]/(x^4+x+1)$	Kurzdarstellung
$[0]$	0000
$[1]$	0001
$[x]$	0010
$[x+1]$	0011
$[x^2]$	0100
$[x^2+1]$	0101
$[x^2+x]$	0110
$[x^2+x+1]$	0111
$[x^3]$	1000
$[x^3+1]$	1001
$[x^3+x]$	1010
$[x^3+x+1]$	1010
$[x^3+x^2]$	1100
$[x^3+x^2+1]$	1101
$[x^3+x^2+x]$	1110
$[x^3+x^2+x+1]$	1111

BEISPIEL: $\pi(x) = x^4 + x + 1 \quad \longleftrightarrow \quad \pi = 10011$

$a(x) = x^3 + x \quad \longleftrightarrow \quad a = 01010$

$b(x) = x^3 + x^2 + 1 \quad \longleftrightarrow \quad b = 01101$

Berechnung von $a(x) \cdot b(x)$ mod $\pi(x)$:

To do	**Realisierung**	**Ergebnis**
Berechne $a(x) \cdot b_3$	$b_3 = 1$, also $a \cdot b_3 = a$	01010
Multipliziere mit x	Shift nach links	10100
Berechne Rest mod $\pi(x)$	**XOR** mit $\pi = 10011$	00111
Addiere $a(x) \cdot b_2$	$b_2 = 1$, also **XOR** mit $a = 01010$	01101
Multipliziere mit x	Shift nach links	11010
Berechne Rest mod $\pi(x)$	**XOR** mit $\pi = 10011$	01001
Addiere $a(x) \cdot b_1$	$b_1 = 0 \;\Rightarrow$ Schritt entfällt	
Multipliziere mit x	Shift nach links	10010
Berechne Rest mod $\pi(x)$	**XOR** mit $\pi = 10011$	00001
Addiere $a(x) \cdot b_0$	$b_0 = 1$, also **XOR** mit $a = 01010$	01011

Ergebnis: $[a(x)] \cdot_\pi [b(x)] = [x^3 + x + 1]$.

$x^2 + 1$ ist ein primitives Element in $\mathbb{Z}_2[x]/(x^4 + x + 1)$:

Tabelle T_1: $T_1[k]$:= Kurzdarstellung von $(x^2 + 1)^k$

Tabelle T_2: $T_2[a_3a_2a_1a_0]$:= k so dass Kurzdarstellung von $(x^2 + 1)^k = a_3a_2a_1a_0$

$T_1[1] = 0101$	$T_2[0001] = 15$
$T_1[2] = 0010$	$T_2[0010] = 2$
$T_1[3] = 1010$	$T_2[0011] = 8$
$T_1[4] = 0100$	$T_2[0100] = 4$
$T_1[5] = 0111$	$T_2[0101] = 1$
$T_1[6] = 1000$	$T_2[0110] = 10$
$T_1[7] = 1110$	$T_2[0111] = 5$
$T_1[8] = 0011$	$T_2[1000] = 6$
$T_1[9] = 1111$	$T_2[1001] = 13$
$T_1[10] = 0110$	$T_2[1010] = 3$
$T_1[11] = 1101$	$T_2[1011] = 14$
$T_1[12] = 1100$	$T_2[1100] = 12$
$T_1[13] = 1001$	$T_2[1101] = 11$
$T_1[14] = 1011$	$T_2[1110] = 7$
$T_1[15] = 0001$	$T_2[1111] = 9$

$[a(x)]\cdot_\pi[b(x)] = [x^3{+}x]\cdot_\pi[x^3{+}x^2{+}1] = [x^3{+}x{+}1]$, denn $T_1(T_2(1010){+}T_2(1101) \bmod 16) = T_1(3{+}11) = 1011.$

In Matrixform:

$$\begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \dots & \alpha^{2t+k-1} \\ 1 & \alpha^2 & \alpha^4 & \alpha^3 & \dots & \alpha^{2(2t+k-1)} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \dots & \alpha^{3(2t+k-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{2t} & \alpha^{4t} & \alpha^{6t} & \dots & \alpha^{2t(2t+k-1)} \end{pmatrix} \cdot \begin{pmatrix} e_1 \\ e_2 \\ e_3 \\ \vdots \\ e_{2t+k-1} \\ e_{2t+k} \end{pmatrix} = \begin{pmatrix} f(\alpha) \\ f(\alpha^2) \\ f(\alpha^3) \\ \vdots \\ f(\alpha^{2t}) \end{pmatrix}.$$

Nehmen wir nun an, daß nur r der e_i's ungleich Null sind, sagen wir $e_{i_1}, e_{i_2}, \dots, e_{i_r}$. Dann können wir dies umschreiben zu

$$\begin{pmatrix} \alpha^{i_1} & \alpha^{i_2} & \dots & \alpha^{i_r} \\ \alpha^{2i_1} & \alpha^{2i_2} & \dots & \alpha^{2i_r} \\ \alpha^{3i_1} & \alpha^{3i_2} & \dots & \alpha^{3i_r} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^{2ti_1} & \alpha^{2ti_2} & \dots & \alpha^{2ti_r} \end{pmatrix} \cdot \begin{pmatrix} e_{i_1} \\ e_{i_2} \\ \vdots \\ e_{i_r} \end{pmatrix} = \begin{pmatrix} f(\alpha) \\ f(\alpha^2) \\ f(\alpha^3) \\ \vdots \\ f(\alpha^{2t}) \end{pmatrix}. \tag{1}$$

Wdh. (Lineare Algebra): Für die Determinante der Vandermonde-Matrix gilt

$$\left| \begin{pmatrix} 1 & 1 & \dots & 1 \\ x_1 & x_2 & \dots & x_r \\ x_1^2 & x_2^2 & \dots & x_r^2 \\ \vdots & \vdots & \ddots & \vdots \\ x_1^{r-1} & x_2^{r-1} & \dots & x_r^{r-1} \end{pmatrix} \right| = \prod_{1 \le i < j \le r} (x_j - x_i).$$

Setzen wir $x_i = \alpha^{i_1}$, so folgt, dass die Matrix in Gleichung (1) vollen Spaltenrang hat, wenn immer $r \le 2t$ ist. (Hier verwenden wir, dass α ein primitives Element in $GF(2^s)$ ist und dass daher $\alpha^j - \alpha^i \neq 0$ für alle $1 \le i < j \le 2^s - 1$.)