KONEČNÁ TĚLESA

PAVEL JAHODA

Prezentace pro přednášku v rámci matematického semináře DiMaS.

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ
Svět vědy CZ 1.07/2.3.00/35.0018

- **Cíl:**

- **Cíl:** Vytvořit množinu dokonalých rozdílů o $p^n + 1$ prvcích.

- **Cíl:** Vytvořit množinu dokonalých rozdílů o $p^n + 1$ prvcích.
- **Prostředky:**

- **Cíl:** Vytvořit množinu dokonalých rozdílů o $p^n + 1$ prvcích.
- **Prostředky:**
  - **Primititivní ireducibilní polynom 3. stupně nad** $GF(p^n)$**.**

- **Cíl:** Vytvořit množinu dokonalých rozdílů o $p^n + 1$ prvcích.
- **Prostředky:**
  - **Primititivní ireducibilní polynom 3. stupně nad** $GF(p^n)$**.**
  - **Tabulka sčítání a násobení v** $GF(p^n)$**.**

Př.:

Př.:

Vytvořte p.d.s. o $5^1 + 1$ prvcích.

Př.:

Vytvořte p.d.s. o $5^1 + 1$ prvcích.
Budeme potřebovat primitivní ireducibilní polynom třetího stupně nad $GF(5^1) = \mathbb{Z}_5$

Př.:

Vytvořte p.d.s. o $5^1 + 1$ prvcích.
Budeme potřebovat primitivní ireducibilní polynom třetího stupně nad $GF(5^1) = \mathbb{Z}_5$
Například:

$$\mathbf{x^3 + x + 1}$$

Př.:

Vytvořte p.d.s. o $5^1 + 1$ prvcích.
Budeme potřebovat primitivní ireducibilní polynom třetího stupně nad $GF(5^1) = \mathbb{Z}_5$
Například:

$$\mathbf{x^3 + x + 1}$$

Prvky z $GF(5^3)$ potom můžeme chápat jako prvky ve tvaru

$$a\lambda^2 + b\lambda + c,$$

kde $a, b, c \in GF(5^1) = \mathbb{Z}_5$ a

Př.:

Vytvořte p.d.s. o $5^1 + 1$ prvcích.
Budeme potřebovat primitivní ireducibilní polynom třetího stupně nad $GF(5^1) = \mathbb{Z}_5$
Například:

$$\mathbf{x^3 + x + 1}$$

Prvky z $GF(5^3)$ potom můžeme chápat jako prvky ve tvaru

$$a\lambda^2 + b\lambda + c,$$

kde $a, b, c \in GF(5^1) = \mathbb{Z}_5$ a λ splňuje podmínku

$$\lambda^3 + \lambda + 1 = 0 \in \mathbf{GF(5^3)}$$

Násobení a sčítání v $GF(5^1) = \mathbb{Z}_5$

$+$	**0**	**1**	**2**	**3**	**4**
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot$	**0**	**1**	**2**	**3**	**4**
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Určíme mocniny prvku λ

Určíme mocniny prvku λ

$$\lambda^i = x_1\lambda^2 + x_2\lambda + x_3$$

Určíme mocniny prvku λ

$$\lambda^i = x_1\lambda^2 + x_2\lambda + x_3$$

$$\lambda^{i+1} = \lambda(x_1\lambda^2 + x_2\lambda + x_3)$$

Určíme mocniny prvku λ

$$\lambda^i = x_1\lambda^2 + x_2\lambda + x_3$$

$$\begin{aligned} \lambda^{i+1} &= \lambda(x_1\lambda^2 + x_2\lambda + x_3) \\ \lambda^{i+1} &= x_1\lambda^3 + x_2\lambda^2 + x_3\lambda \end{aligned}$$

Určíme mocniny prvku λ

$$\lambda^i = x_1\lambda^2 + x_2\lambda + x_3$$

$$\begin{aligned} \lambda^{i+1} &= \lambda(x_1\lambda^2 + x_2\lambda + x_3) \\ \lambda^{i+1} &= x_1\lambda^3 + x_2\lambda^2 + x_3\lambda - x_1 \underbrace{(\lambda^3 + \lambda + 1)}_{=0} \end{aligned}$$

Určíme mocniny prvku λ

$$\lambda^i = x_1\lambda^2 + x_2\lambda + x_3$$

$$\begin{aligned}
\lambda^{i+1} &= \lambda(x_1\lambda^2 + x_2\lambda + x_3) \\
\lambda^{i+1} &= x_1\lambda^3 + x_2\lambda^2 + x_3\lambda - x_1 \underbrace{(\lambda^3 + \lambda + 1)}_{=0} \\
\lambda^{i+1} &= x_2\lambda^2 + (x_3 - x_1)\lambda - x_1
\end{aligned}$$

Určíme mocniny prvku λ

$$\lambda^i = x_1\lambda^2 + x_2\lambda + x_3$$

$$\begin{aligned}
\lambda^{i+1} &= \lambda(x_1\lambda^2 + x_2\lambda + x_3) \\
\lambda^{i+1} &= x_1\lambda^3 + x_2\lambda^2 + x_3\lambda - x_1 \underbrace{(\lambda^3 + \lambda + 1)}_{=0} \\
\lambda^{i+1} &= x_2\lambda^2 + (x_3 - x_1)\lambda - x_1
\end{aligned}$$

Určíme mocniny prvku λ

$$\lambda^i = x_1\lambda^2 + x_2\lambda + x_3$$

$$\begin{aligned}
\lambda^{i+1} &= \lambda(x_1\lambda^2 + x_2\lambda + x_3) \\
\lambda^{i+1} &= x_1\lambda^3 + x_2\lambda^2 + x_3\lambda - x_1 \underbrace{(\lambda^3 + \lambda + 1)}_{=0} \\
\lambda^{i+1} &= x_2\lambda^2 + (x_3 - x_1)\lambda - x_1
\end{aligned}$$

Souřadnicový zápis: $\lambda^i = (x_1, x_2, x_3) \Rightarrow$

Určíme mocniny prvku λ

$$\lambda^i = x_1\lambda^2 + x_2\lambda + x_3$$

$$\begin{aligned}
\lambda^{i+1} &= \lambda(x_1\lambda^2 + x_2\lambda + x_3) \\
\lambda^{i+1} &= x_1\lambda^3 + x_2\lambda^2 + x_3\lambda - x_1 \underbrace{(\lambda^3 + \lambda + 1)}_{=0} \\
\lambda^{i+1} &= x_2\lambda^2 + (x_3 - x_1)\lambda - x_1
\end{aligned}$$

Souřadnicový zápis: $\lambda^i = (x_1, x_2, x_3) \Rightarrow \lambda^{i+1} = (x_2, x_3 - x_1, -x_1)$.

Mocniny prvku λ - určujeme, dokud nenajdeme $5^1 + 1$ mocnin, jejichž první souřadnice je rovna nule. Souřadnicový zápis:
$\lambda^i = (x_1, x_2, x_3) \Rightarrow \lambda^{i+1} = (x_2, x_3 - x_1, -x_1)$.

Mocniny prvku λ - určujeme, dokud nenajdeme $5^1 + 1$ mocnin, jejichž první souřadnice je rovna nule. Souřadnicový zápis:
$\lambda^i = (x_1, x_2, x_3) \Rightarrow \lambda^{i+1} = (x_2, x_3 - x_1, -x_1)$.

$$\lambda^0 \quad = \quad (\quad 0 \quad , \quad 0 \quad , \quad 1 \quad)$$

Mocniny prvku λ - určujeme, dokud nenajdeme $5^1 + 1$ mocnin, jejichž první souřadnice je rovna nule. Souřadnicový zápis:
$\lambda^i = (x_1, x_2, x_3) \Rightarrow \lambda^{i+1} = (x_2, x_3 - x_1, -x_1)$.

$$\begin{array}{lcccccc} \lambda^0 & = & (& 0 & , & 0 & , & 1 &) \\ \lambda^1 & = & (& 0 & , & 1 & , & 0 &) \end{array}$$

Mocniny prvku λ - určujeme, dokud nenajdeme $5^1 + 1$ mocnin, jejichž první souřadnice je rovna nule. Souřadnicový zápis:
$\lambda^i = (x_1, x_2, x_3) \Rightarrow \lambda^{i+1} = (x_2, x_3 - x_1, -x_1)$.

$$\begin{array}{lcccccc} \lambda^0 & = & (& 0 & , & 0 & , & 1 &) \\ \lambda^1 & = & (& 0 & , & 1 & , & 0 &) \\ \lambda^2 & = & (& 1 & , & 0 & , & 0 &) \end{array}$$

Mocniny prvku λ - určujeme, dokud nenajdeme $5^1 + 1$ mocnin, jejichž první souřadnice je rovna nule. Souřadnicový zápis:
$\lambda^i = (x_1, x_2, x_3) \Rightarrow \lambda^{i+1} = (x_2, x_3 - x_1, -x_1)$.

$$\begin{array}{lcccccc} \lambda^0 & = & (& 0 & , & 0 & , & 1 &) \\ \lambda^1 & = & (& 0 & , & 1 & , & 0 &) \\ \lambda^2 & = & (& 1 & , & 0 & , & 0 &) \\ \lambda^3 & = & (& 0 & , & -1 & , & -1 &) \end{array}$$

Mocniny prvku λ - určujeme, dokud nenajdeme $5^1 + 1$ mocnin, jejichž první souřadnice je rovna nule. Souřadnicový zápis:
$\lambda^i = (x_1, x_2, x_3) \Rightarrow \lambda^{i+1} = (x_2, x_3 - x_1, -x_1)$.

$$
\begin{array}{lcccccccc}
\lambda^0 & = & (& 0 & , & 0 & , & 1 &) \\
\lambda^1 & = & (& 0 & , & 1 & , & 0 &) \\
\lambda^2 & = & (& 1 & , & 0 & , & 0 &) \\
\lambda^3 & = & (& 0 & , & -1 & , & -1 &) \\
\lambda^4 & = & (& -1 & , & -1 & , & 0 &)
\end{array}
$$

Mocniny prvku λ - určujeme, dokud nenajdeme $5^1 + 1$ mocnin, jejichž první souřadnice je rovna nule. Souřadnicový zápis:
$\lambda^i = (x_1, x_2, x_3) \Rightarrow \lambda^{i+1} = (x_2, x_3 - x_1, -x_1)$.

$$
\begin{array}{lcccccccc}
\lambda^0 & = & (& 0 & , & 0 & , & 1 &) \\
\lambda^1 & = & (& 0 & , & 1 & , & 0 &) \\
\lambda^2 & = & (& 1 & , & 0 & , & 0 &) \\
\lambda^3 & = & (& 0 & , & -1 & , & -1 &) \\
\lambda^4 & = & (& -1 & , & -1 & , & 0 &) \\
\lambda^5 & = & (& -1 & , & 1 & , & 1 &)
\end{array}
$$

Mocniny prvku λ - určujeme, dokud nenajdeme $5^1 + 1$ mocnin, jejichž první souřadnice je rovna nule. Souřadnicový zápis:
$\lambda^i = (x_1, x_2, x_3) \Rightarrow \lambda^{i+1} = (x_2, x_3 - x_1, -x_1)$.

$$
\begin{array}{lcccccc}
\lambda^0 & = & (& 0 & , & 0 & , & 1 &) \\
\lambda^1 & = & (& 0 & , & 1 & , & 0 &) \\
\lambda^2 & = & (& 1 & , & 0 & , & 0 &) \\
\lambda^3 & = & (& 0 & , & -1 & , & -1 &) \\
\lambda^4 & = & (& -1 & , & -1 & , & 0 &) \\
\lambda^5 & = & (& -1 & , & 1 & , & 1 &) \\
\lambda^6 & = & (& 1 & , & 2 & , & 1 &)
\end{array}
$$

Mocniny prvku λ - určujeme, dokud nenajdeme $5^1 + 1$ mocnin, jejichž první souřadnice je rovna nule. Souřadnicový zápis:
$\lambda^i = (x_1, x_2, x_3) \Rightarrow \lambda^{i+1} = (x_2, x_3 - x_1, -x_1)$.

$$
\begin{array}{lcccccc}
\lambda^0 & = & (& 0 & , & 0 & , & 1 &) \\
\lambda^1 & = & (& 0 & , & 1 & , & 0 &) \\
\lambda^2 & = & (& 1 & , & 0 & , & 0 &) \\
\lambda^3 & = & (& 0 & , & -1 & , & -1 &) \\
\lambda^4 & = & (& -1 & , & -1 & , & 0 &) \\
\lambda^5 & = & (& -1 & , & 1 & , & 1 &) \\
\lambda^6 & = & (& 1 & , & 2 & , & 1 &) \\
\lambda^7 & = & (& 2 & , & 0 & , & -1 &)
\end{array}
$$

Mocniny prvku λ - určujeme, dokud nenajdeme $5^1 + 1$ mocnin, jejichž první souřadnice je rovna nule. Souřadnicový zápis:
$\lambda^i = (x_1, x_2, x_3) \Rightarrow \lambda^{i+1} = (x_2, x_3 - x_1, -x_1)$.

$$
\begin{array}{lcccccc}
\lambda^0 & = & (& 0 & , & 0 & , & 1 &) \\
\lambda^1 & = & (& 0 & , & 1 & , & 0 &) \\
\lambda^2 & = & (& 1 & , & 0 & , & 0 &) \\
\lambda^3 & = & (& 0 & , & -1 & , & -1 &) \\
\lambda^4 & = & (& -1 & , & -1 & , & 0 &) \\
\lambda^5 & = & (& -1 & , & 1 & , & 1 &) \\
\lambda^6 & = & (& 1 & , & 2 & , & 1 &) \\
\lambda^7 & = & (& 2 & , & 0 & , & -1 &) \\
\lambda^8 & = & (& 0 & , & -3 & , & -2 &)
\end{array}
$$

Mocniny prvku λ - určujeme, dokud nenajdeme $5^1 + 1$ mocnin, jejichž první souřadnice je rovna nule. Souřadnicový zápis:
$\lambda^i = (x_1, x_2, x_3) \Rightarrow \lambda^{i+1} = (x_2, x_3 - x_1, -x_1)$.

$$
\begin{array}{lcccccc}
\lambda^0 & = & (& 0 & , & 0 & , & 1 &) \\
\lambda^1 & = & (& 0 & , & 1 & , & 0 &) \\
\lambda^2 & = & (& 1 & , & 0 & , & 0 &) \\
\lambda^3 & = & (& 0 & , & -1 & , & -1 &) \\
\lambda^4 & = & (& -1 & , & -1 & , & 0 &) \\
\lambda^5 & = & (& -1 & , & 1 & , & 1 &) \\
\lambda^6 & = & (& 1 & , & 2 & , & 1 &) \\
\lambda^7 & = & (& 2 & , & 0 & , & -1 &) \\
\lambda^8 & = & (& 0 & , & -3 & , & -2 &) \\
\lambda^9 & = & (& -3 & , & -2 & , & 0 &)
\end{array}
$$

Mocniny prvku λ - určujeme, dokud nenajdeme $5^1 + 1$ mocnin, jejichž první souřadnice je rovna nule. Souřadnicový zápis:
$\lambda^i = (x_1, x_2, x_3) \Rightarrow \lambda^{i+1} = (x_2, x_3 - x_1, -x_1)$.

$$
\begin{array}{lcccccc}
\lambda^0 & = & (& 0 & , & 0 & , & 1 &) \\
\lambda^1 & = & (& 0 & , & 1 & , & 0 &) \\
\lambda^2 & = & (& 1 & , & 0 & , & 0 &) \\
\lambda^3 & = & (& 0 & , & -1 & , & -1 &) \\
\lambda^4 & = & (& -1 & , & -1 & , & 0 &) \\
\lambda^5 & = & (& -1 & , & 1 & , & 1 &) \\
\lambda^6 & = & (& 1 & , & 2 & , & 1 &) \\
\lambda^7 & = & (& 2 & , & 0 & , & -1 &) \\
\lambda^8 & = & (& 0 & , & -3 & , & -2 &) \\
\lambda^9 & = & (& -3 & , & -2 & , & 0 &) \\
\lambda^{10} & = & (& -2 & , & 3 & , & 3 &)
\end{array}
$$

Mocniny prvku λ - určujeme, dokud nenajdeme $5^1 + 1$ mocnin, jejichž první souřadnice je rovna nule. Souřadnicový zápis:
$\lambda^i = (x_1, x_2, x_3) \Rightarrow \lambda^{i+1} = (x_2, x_3 - x_1, -x_1)$.

$$
\begin{array}{lcccccc}
\lambda^0 & = & (& 0 & , & 0 & , & 1 &) \\
\lambda^1 & = & (& 0 & , & 1 & , & 0 &) \\
\lambda^2 & = & (& 1 & , & 0 & , & 0 &) \\
\lambda^3 & = & (& 0 & , & -1 & , & -1 &) \\
\lambda^4 & = & (& -1 & , & -1 & , & 0 &) \\
\lambda^5 & = & (& -1 & , & 1 & , & 1 &) \\
\lambda^6 & = & (& 1 & , & 2 & , & 1 &) \\
\lambda^7 & = & (& 2 & , & 0 & , & -1 &) \\
\lambda^8 & = & (& 0 & , & -3 & , & -2 &) \\
\lambda^9 & = & (& -3 & , & -2 & , & 0 &) \\
\lambda^{10} & = & (& -2 & , & 3 & , & 3 &) \\
\lambda^{11} & = & (& 3 & , & 0 & , & 2 &)
\end{array}
$$

Mocniny prvku λ - určujeme, dokud nenajdeme $5^1 + 1$ mocnin, jejichž první souřadnice je rovna nule. Souřadnicový zápis:
$\lambda^i = (x_1, x_2, x_3) \Rightarrow \lambda^{i+1} = (x_2, x_3 - x_1, -x_1)$.

$$
\begin{array}{lcccccc}
\lambda^0 & = & (& 0 & , & 0 & , & 1 &) \\
\lambda^1 & = & (& 0 & , & 1 & , & 0 &) \\
\lambda^2 & = & (& 1 & , & 0 & , & 0 &) \\
\lambda^3 & = & (& 0 & , & -1 & , & -1 &) \\
\lambda^4 & = & (& -1 & , & -1 & , & 0 &) \\
\lambda^5 & = & (& -1 & , & 1 & , & 1 &) \\
\lambda^6 & = & (& 1 & , & 2 & , & 1 &) \\
\lambda^7 & = & (& 2 & , & 0 & , & -1 &) \\
\lambda^8 & = & (& 0 & , & -3 & , & -2 &) \\
\lambda^9 & = & (& -3 & , & -2 & , & 0 &) \\
\lambda^{10} & = & (& -2 & , & 3 & , & 3 &) \\
\lambda^{11} & = & (& 3 & , & 0 & , & 2 &) \\
\lambda^{12} & = & (& 0 & , & -1 & , & -3 &)
\end{array}
$$

Mocniny prvku λ - určujeme, dokud nenajdeme $5^1 + 1$ mocnin, jejichž první souřadnice je rovna nule. Souřadnicový zápis:
$\lambda^i = (x_1, x_2, x_3) \Rightarrow \lambda^{i+1} = (x_2, x_3 - x_1, -x_1)$.

$$
\begin{array}{lcccccc}
\lambda^0 & = & (& 0 & , & 0 & , & 1 &) \\
\lambda^1 & = & (& 0 & , & 1 & , & 0 &) \\
\lambda^2 & = & (& 1 & , & 0 & , & 0 &) \\
\lambda^3 & = & (& 0 & , & -1 & , & -1 &) \\
\lambda^4 & = & (& -1 & , & -1 & , & 0 &) \\
\lambda^5 & = & (& -1 & , & 1 & , & 1 &) \\
\lambda^6 & = & (& 1 & , & 2 & , & 1 &) \\
\lambda^7 & = & (& 2 & , & 0 & , & -1 &) \\
\lambda^8 & = & (& 0 & , & -3 & , & -2 &) \\
\lambda^9 & = & (& -3 & , & -2 & , & 0 &) \\
\lambda^{10} & = & (& -2 & , & 3 & , & 3 &) \\
\lambda^{11} & = & (& 3 & , & 0 & , & 2 &) \\
\lambda^{12} & = & (& 0 & , & -1 & , & -3 &) \\
\lambda^{13} & = & (& -1 & , & -3 & , & 0 &)
\end{array}
$$

Mocniny prvku λ - určujeme, dokud nenajdeme $5^1 + 1$ mocnin, jejichž první souřadnice je rovna nule. Souřadnicový zápis:
$\lambda^i = (x_1, x_2, x_3) \Rightarrow \lambda^{i+1} = (x_2, x_3 - x_1, -x_1)$.

$$
\begin{array}{lcccccc}
\lambda^0 & = & (& 0 & , & 0 & , & 1 &) \\
\lambda^1 & = & (& 0 & , & 1 & , & 0 &) \\
\lambda^2 & = & (& 1 & , & 0 & , & 0 &) \\
\lambda^3 & = & (& 0 & , & -1 & , & -1 &) \\
\lambda^4 & = & (& -1 & , & -1 & , & 0 &) \\
\lambda^5 & = & (& -1 & , & 1 & , & 1 &) \\
\lambda^6 & = & (& 1 & , & 2 & , & 1 &) \\
\lambda^7 & = & (& 2 & , & 0 & , & -1 &) \\
\lambda^8 & = & (& 0 & , & -3 & , & -2 &) \\
\lambda^9 & = & (& -3 & , & -2 & , & 0 &) \\
\lambda^{10} & = & (& -2 & , & 3 & , & 3 &) \\
\lambda^{11} & = & (& 3 & , & 0 & , & 2 &) \\
\lambda^{12} & = & (& 0 & , & -1 & , & -3 &) \\
\lambda^{13} & = & (& -1 & , & -3 & , & 0 &) \\
\lambda^{14} & = & (& -3 & , & 1 & , & 1 &)
\end{array}
$$

Mocniny prvku λ - určujeme, dokud nenajdeme $5^1 + 1$ mocnin, jejichž první souřadnice je rovna nule. Souřadnicový zápis:
$\lambda^i = (x_1, x_2, x_3) \Rightarrow \lambda^{i+1} = (x_2, x_3 - x_1, -x_1)$.

$$
\begin{array}{lcccccc}
\lambda^0 & = & (& 0 & , & 0 & , & 1 &) \\
\lambda^1 & = & (& 0 & , & 1 & , & 0 &) \\
\lambda^2 & = & (& 1 & , & 0 & , & 0 &) \\
\lambda^3 & = & (& 0 & , & -1 & , & -1 &) \\
\lambda^4 & = & (& -1 & , & -1 & , & 0 &) \\
\lambda^5 & = & (& -1 & , & 1 & , & 1 &) \\
\lambda^6 & = & (& 1 & , & 2 & , & 1 &) \\
\lambda^7 & = & (& 2 & , & 0 & , & -1 &) \\
\lambda^8 & = & (& 0 & , & -3 & , & -2 &) \\
\lambda^9 & = & (& -3 & , & -2 & , & 0 &) \\
\lambda^{10} & = & (& -2 & , & 3 & , & 3 &) \\
\lambda^{11} & = & (& 3 & , & 0 & , & 2 &) \\
\lambda^{12} & = & (& 0 & , & -1 & , & -3 &) \\
\lambda^{13} & = & (& -1 & , & -3 & , & 0 &) \\
\lambda^{14} & = & (& -3 & , & 1 & , & 1 &) \\
\lambda^{15} & = & (& 1 & , & 4 & , & 3 &)
\end{array}
$$

Mocniny prvku λ - určujeme, dokud nenajdeme $5^1 + 1$ mocnin, jejichž první souřadnice je rovna nule. Souřadnicový zápis:
$\lambda^i = (x_1, x_2, x_3) \Rightarrow \lambda^{i+1} = (x_2, x_3 - x_1, -x_1)$.

$$
\begin{array}{lcccccc}
\lambda^0 & = & (& 0 & , & 0 & , & 1 &) \\
\lambda^1 & = & (& 0 & , & 1 & , & 0 &) \\
\lambda^2 & = & (& 1 & , & 0 & , & 0 &) \\
\lambda^3 & = & (& 0 & , & -1 & , & -1 &) \\
\lambda^4 & = & (& -1 & , & -1 & , & 0 &) \\
\lambda^5 & = & (& -1 & , & 1 & , & 1 &) \\
\lambda^6 & = & (& 1 & , & 2 & , & 1 &) \\
\lambda^7 & = & (& 2 & , & 0 & , & -1 &) \\
\lambda^8 & = & (& 0 & , & -3 & , & -2 &) \\
\lambda^9 & = & (& -3 & , & -2 & , & 0 &) \\
\lambda^{10} & = & (& -2 & , & 3 & , & 3 &) \\
\lambda^{11} & = & (& 3 & , & 0 & , & 2 &) \\
\lambda^{12} & = & (& 0 & , & -1 & , & -3 &) \\
\lambda^{13} & = & (& -1 & , & -3 & , & 0 &) \\
\lambda^{14} & = & (& -3 & , & 1 & , & 1 &) \\
\lambda^{15} & = & (& 1 & , & 4 & , & 3 &) \\
\lambda^{16} & = & (& 4 & , & 2 & , & -1 &)
\end{array}
$$

Mocniny prvku λ - určujeme, dokud nenajdeme $5^1 + 1$ mocnin, jejichž první souřadnice je rovna nule. Souřadnicový zápis:
$\lambda^i = (x_1, x_2, x_3) \Rightarrow \lambda^{i+1} = (x_2, x_3 - x_1, -x_1)$.

$$
\begin{array}{lcccccc}
\lambda^0 & = & (& 0 & , & 0 & , & 1 &) \\
\lambda^1 & = & (& 0 & , & 1 & , & 0 &) \\
\lambda^2 & = & (& 1 & , & 0 & , & 0 &) \\
\lambda^3 & = & (& 0 & , & -1 & , & -1 &) \\
\lambda^4 & = & (& -1 & , & -1 & , & 0 &) \\
\lambda^5 & = & (& -1 & , & 1 & , & 1 &) \\
\lambda^6 & = & (& 1 & , & 2 & , & 1 &) \\
\lambda^7 & = & (& 2 & , & 0 & , & -1 &) \\
\lambda^8 & = & (& 0 & , & -3 & , & -2 &) \\
\lambda^9 & = & (& -3 & , & -2 & , & 0 &) \\
\lambda^{10} & = & (& -2 & , & 3 & , & 3 &) \\
\lambda^{11} & = & (& 3 & , & 0 & , & 2 &) \\
\lambda^{12} & = & (& 0 & , & -1 & , & -3 &) \\
\lambda^{13} & = & (& -1 & , & -3 & , & 0 &) \\
\lambda^{14} & = & (& -3 & , & 1 & , & 1 &) \\
\lambda^{15} & = & (& 1 & , & 4 & , & 3 &) \\
\lambda^{16} & = & (& 4 & , & 2 & , & -1 &) \\
\lambda^{17} & = & (& 2 & , & 0 & , & -4 &)
\end{array}
$$

Mocniny prvku λ - určujeme, dokud nenajdeme $5^1 + 1$ mocnin, jejichž první souřadnice je rovna nule. Souřadnicový zápis:
$\lambda^i = (x_1, x_2, x_3) \Rightarrow \lambda^{i+1} = (x_2, x_3 - x_1, -x_1)$.

$$
\begin{array}{lcccccc}
\lambda^{0} & = & (& 0 & , & 0 & , & 1 &) \\
\lambda^{1} & = & (& 0 & , & 1 & , & 0 &) \\
\lambda^{2} & = & (& 1 & , & 0 & , & 0 &) \\
\lambda^{3} & = & (& 0 & , & -1 & , & -1 &) \\
\lambda^{4} & = & (& -1 & , & -1 & , & 0 &) \\
\lambda^{5} & = & (& -1 & , & 1 & , & 1 &) \\
\lambda^{6} & = & (& 1 & , & 2 & , & 1 &) \\
\lambda^{7} & = & (& 2 & , & 0 & , & -1 &) \\
\lambda^{8} & = & (& 0 & , & -3 & , & -2 &) \\
\lambda^{9} & = & (& -3 & , & -2 & , & 0 &) \\
\lambda^{10} & = & (& -2 & , & 3 & , & 3 &) \\
\lambda^{11} & = & (& 3 & , & 0 & , & 2 &) \\
\lambda^{12} & = & (& 0 & , & -1 & , & -3 &) \\
\lambda^{13} & = & (& -1 & , & -3 & , & 0 &) \\
\lambda^{14} & = & (& -3 & , & 1 & , & 1 &) \\
\lambda^{15} & = & (& 1 & , & 4 & , & 3 &) \\
\lambda^{16} & = & (& 4 & , & 2 & , & -1 &) \\
\lambda^{17} & = & (& 2 & , & 0 & , & -4 &) \\
\lambda^{18} & = & (& 0 & , & -1 & , & -2 &)
\end{array}
$$

Mocniny prvku λ - určujeme, dokud nenajdeme $5^1 + 1$ mocnin, jejichž první souřadnice je rovna nule. Souřadnicový zápis:
$\lambda^i = (x_1, x_2, x_3) \Rightarrow \lambda^{i+1} = (x_2, x_3 - x_1, -x_1)$.

$$
\begin{array}{lcccccc}
\lambda^{0} & = & (& 0 & , & 0 & , & 1 &) \\
\lambda^{1} & = & (& 0 & , & 1 & , & 0 &) \\
\lambda^{2} & = & (& 1 & , & 0 & , & 0 &) \\
\lambda^{3} & = & (& 0 & , & -1 & , & -1 &) \\
\lambda^{4} & = & (& -1 & , & -1 & , & 0 &) \\
\lambda^{5} & = & (& -1 & , & 1 & , & 1 &) \\
\lambda^{6} & = & (& 1 & , & 2 & , & 1 &) \\
\lambda^{7} & = & (& 2 & , & 0 & , & -1 &) \\
\lambda^{8} & = & (& 0 & , & -3 & , & -2 &) \\
\lambda^{9} & = & (& -3 & , & -2 & , & 0 &) \\
\lambda^{10} & = & (& -2 & , & 3 & , & 3 &) \\
\lambda^{11} & = & (& 3 & , & 0 & , & 2 &) \\
\lambda^{12} & = & (& 0 & , & -1 & , & -3 &) \\
\lambda^{13} & = & (& -1 & , & -3 & , & 0 &) \\
\lambda^{14} & = & (& -3 & , & 1 & , & 1 &) \\
\lambda^{15} & = & (& 1 & , & 4 & , & 3 &) \\
\lambda^{16} & = & (& 4 & , & 2 & , & -1 &) \\
\lambda^{17} & = & (& 2 & , & 0 & , & -4 &) \\
\lambda^{18} & = & (& 0 & , & -1 & , & -2 &)
\end{array}
$$

Mocniny prvku λ - určujeme, dokud nenajdeme $5^1 + 1$ mocnin, jejichž první souřadnice je rovna nule. Souřadnicový zápis: $\lambda^i = (x_1, x_2, x_3) \Rightarrow \lambda^{i+1} = (x_2, x_3 - x_1, -x_1)$.

$$
\begin{array}{lcccccc}
\lambda^{0} & = & (& 0 & , & 0 & , & 1 &) \\
\lambda^{1} & = & (& 0 & , & 1 & , & 0 &) \\
\lambda^{2} & = & (& 1 & , & 0 & , & 0 &) \\
\lambda^{3} & = & (& 0 & , & -1 & , & -1 &) \\
\lambda^{4} & = & (& -1 & , & -1 & , & 0 &) \\
\lambda^{5} & = & (& -1 & , & 1 & , & 1 &) \\
\lambda^{6} & = & (& 1 & , & 2 & , & 1 &) \\
\lambda^{7} & = & (& 2 & , & 0 & , & -1 &) \\
\lambda^{8} & = & (& 0 & , & -3 & , & -2 &) \\
\lambda^{9} & = & (& -3 & , & -2 & , & 0 &) \\
\lambda^{10} & = & (& -2 & , & 3 & , & 3 &) \\
\lambda^{11} & = & (& 3 & , & 0 & , & 2 &) \\
\lambda^{12} & = & (& 0 & , & -1 & , & -3 &) \\
\lambda^{13} & = & (& -1 & , & -3 & , & 0 &) \\
\lambda^{14} & = & (& -3 & , & 1 & , & 1 &) \\
\lambda^{15} & = & (& 1 & , & 4 & , & 3 &) \\
\lambda^{16} & = & (& 4 & , & 2 & , & -1 &) \\
\lambda^{17} & = & (& 2 & , & 0 & , & -4 &) \\
\lambda^{18} & = & (& 0 & , & -1 & , & -2 &)
\end{array}
$$

Mocniny prvku λ - určujeme, dokud nenajdeme $5^1 + 1$ mocnin, jejichž první souřadnice je rovna nule. Souřadnicový zápis: $\lambda^i = (x_1, x_2, x_3) \Rightarrow \lambda^{i+1} = (x_2, x_3 - x_1, -x_1)$.

$$
\begin{array}{lcccccc}
\lambda^{0} & = & (& 0 & , & 0 & , & 1 &) \\
\lambda^{1} & = & (& 0 & , & 1 & , & 0 &) \\
\lambda^{2} & = & (& 1 & , & 0 & , & 0 &) \\
\lambda^{3} & = & (& 0 & , & -1 & , & -1 &) \\
\lambda^{4} & = & (& -1 & , & -1 & , & 0 &) \\
\lambda^{5} & = & (& -1 & , & 1 & , & 1 &) \\
\lambda^{6} & = & (& 1 & , & 2 & , & 1 &) \\
\lambda^{7} & = & (& 2 & , & 0 & , & -1 &) \\
\lambda^{8} & = & (& 0 & , & -3 & , & -2 &) \\
\lambda^{9} & = & (& -3 & , & -2 & , & 0 &) \\
\lambda^{10} & = & (& -2 & , & 3 & , & 3 &) \\
\lambda^{11} & = & (& 3 & , & 0 & , & 2 &) \\
\lambda^{12} & = & (& 0 & , & -1 & , & -3 &) \\
\lambda^{13} & = & (& -1 & , & -3 & , & 0 &) \\
\lambda^{14} & = & (& -3 & , & 1 & , & 1 &) \\
\lambda^{15} & = & (& 1 & , & 4 & , & 3 &) \\
\lambda^{16} & = & (& 4 & , & 2 & , & -1 &) \\
\lambda^{17} & = & (& 2 & , & 0 & , & -4 &) \\
\lambda^{18} & = & (& 0 & , & -1 & , & -2 &)
\end{array}
$$

Mocniny prvku λ - určujeme, dokud nenajdeme $5^1 + 1$ mocnin, jejichž první souřadnice je rovna nule. Souřadnicový zápis:
$\lambda^i = (x_1, x_2, x_3) \Rightarrow \lambda^{i+1} = (x_2, x_3 - x_1, -x_1)$.

$$
\begin{array}{lcccccc}
\lambda^{0} & = & (& 0 & , & 0 & , & 1 &) \\
\lambda^{1} & = & (& 0 & , & 1 & , & 0 &) \\
\lambda^{2} & = & (& 1 & , & 0 & , & 0 &) \\
\lambda^{3} & = & (& 0 & , & -1 & , & -1 &) \\
\lambda^{4} & = & (& -1 & , & -1 & , & 0 &) \\
\lambda^{5} & = & (& -1 & , & 1 & , & 1 &) \\
\lambda^{6} & = & (& 1 & , & 2 & , & 1 &) \\
\lambda^{7} & = & (& 2 & , & 0 & , & -1 &) \\
\lambda^{8} & = & (& 0 & , & -3 & , & -2 &) \\
\lambda^{9} & = & (& -3 & , & -2 & , & 0 &) \\
\lambda^{10} & = & (& -2 & , & 3 & , & 3 &) \\
\lambda^{11} & = & (& 3 & , & 0 & , & 2 &) \\
\lambda^{12} & = & (& 0 & , & -1 & , & -3 &) \\
\lambda^{13} & = & (& -1 & , & -3 & , & 0 &) \\
\lambda^{14} & = & (& -3 & , & 1 & , & 1 &) \\
\lambda^{15} & = & (& 1 & , & 4 & , & 3 &) \\
\lambda^{16} & = & (& 4 & , & 2 & , & -1 &) \\
\lambda^{17} & = & (& 2 & , & 0 & , & -4 &) \\
\lambda^{18} & = & (& 0 & , & -1 & , & -2 &)
\end{array}
$$

Mocniny prvku λ - určujeme, dokud nenajdeme $5^1 + 1$ mocnin, jejichž první souřadnice je rovna nule. Souřadnicový zápis: $\lambda^i = (x_1, x_2, x_3) \Rightarrow \lambda^{i+1} = (x_2, x_3 - x_1, -x_1)$.

$$
\begin{array}{lcccccc}
\lambda^{0} & = & (& 0 & , & 0 & , & 1 &) \\
\lambda^{1} & = & (& 0 & , & 1 & , & 0 &) \\
\lambda^{2} & = & (& 1 & , & 0 & , & 0 &) \\
\lambda^{3} & = & (& 0 & , & -1 & , & -1 &) \\
\lambda^{4} & = & (& -1 & , & -1 & , & 0 &) \\
\lambda^{5} & = & (& -1 & , & 1 & , & 1 &) \\
\lambda^{6} & = & (& 1 & , & 2 & , & 1 &) \\
\lambda^{7} & = & (& 2 & , & 0 & , & -1 &) \\
\lambda^{8} & = & (& 0 & , & -3 & , & -2 &) \\
\lambda^{9} & = & (& -3 & , & -2 & , & 0 &) \\
\lambda^{10} & = & (& -2 & , & 3 & , & 3 &) \\
\lambda^{11} & = & (& 3 & , & 0 & , & 2 &) \\
\lambda^{12} & = & (& 0 & , & -1 & , & -3 &) \\
\lambda^{13} & = & (& -1 & , & -3 & , & 0 &) \\
\lambda^{14} & = & (& -3 & , & 1 & , & 1 &) \\
\lambda^{15} & = & (& 1 & , & 4 & , & 3 &) \\
\lambda^{16} & = & (& 4 & , & 2 & , & -1 &) \\
\lambda^{17} & = & (& 2 & , & 0 & , & -4 &) \\
\lambda^{18} & = & (& 0 & , & -1 & , & -2 &)
\end{array}
$$

Mocniny prvku λ - určujeme, dokud nenajdeme $5^1 + 1$ mocnin, jejichž první souřadnice je rovna nule. Souřadnicový zápis: $\lambda^i = (x_1, x_2, x_3) \Rightarrow \lambda^{i+1} = (x_2, x_3 - x_1, -x_1)$.

$$
\begin{array}{lcccccc}
\lambda^{0} & = & (& 0 & , & 0 & , & 1 &) \\
\lambda^{1} & = & (& 0 & , & 1 & , & 0 &) \\
\lambda^{2} & = & (& 1 & , & 0 & , & 0 &) \\
\lambda^{3} & = & (& 0 & , & -1 & , & -1 &) \\
\lambda^{4} & = & (& -1 & , & -1 & , & 0 &) \\
\lambda^{5} & = & (& -1 & , & 1 & , & 1 &) \\
\lambda^{6} & = & (& 1 & , & 2 & , & 1 &) \\
\lambda^{7} & = & (& 2 & , & 0 & , & -1 &) \\
\lambda^{8} & = & (& 0 & , & -3 & , & -2 &) \\
\lambda^{9} & = & (& -3 & , & -2 & , & 0 &) \\
\lambda^{10} & = & (& -2 & , & 3 & , & 3 &) \\
\lambda^{11} & = & (& 3 & , & 0 & , & 2 &) \\
\lambda^{12} & = & (& 0 & , & -1 & , & -3 &) \\
\lambda^{13} & = & (& -1 & , & -3 & , & 0 &) \\
\lambda^{14} & = & (& -3 & , & 1 & , & 1 &) \\
\lambda^{15} & = & (& 1 & , & 4 & , & 3 &) \\
\lambda^{16} & = & (& 4 & , & 2 & , & -1 &) \\
\lambda^{17} & = & (& 2 & , & 0 & , & -4 &) \\
\lambda^{18} & = & (& 0 & , & -1 & , & -2 &)
\end{array}
$$

Mocniny prvku λ - určujeme, dokud nenajdeme $5^1 + 1$ mocnin, jejichž první souřadnice je rovna nule. Souřadnicový zápis:
$\lambda^i = (x_1, x_2, x_3) \Rightarrow \lambda^{i+1} = (x_2, x_3 - x_1, -x_1)$.

$$
\begin{array}{lcccccc}
\lambda^{0} & = & (& 0 & , & 0 & , & 1 &) \\
\lambda^{1} & = & (& 0 & , & 1 & , & 0 &) \\
\lambda^{2} & = & (& 1 & , & 0 & , & 0 &) \\
\lambda^{3} & = & (& 0 & , & -1 & , & -1 &) \\
\lambda^{4} & = & (& -1 & , & -1 & , & 0 &) \\
\lambda^{5} & = & (& -1 & , & 1 & , & 1 &) \\
\lambda^{6} & = & (& 1 & , & 2 & , & 1 &) \\
\lambda^{7} & = & (& 2 & , & 0 & , & -1 &) \\
\lambda^{8} & = & (& 0 & , & -3 & , & -2 &) \\
\lambda^{9} & = & (& -3 & , & -2 & , & 0 &) \\
\lambda^{10} & = & (& -2 & , & 3 & , & 3 &) \\
\lambda^{11} & = & (& 3 & , & 0 & , & 2 &) \\
\lambda^{12} & = & (& 0 & , & -1 & , & -3 &) \\
\lambda^{13} & = & (& -1 & , & -3 & , & 0 &) \\
\lambda^{14} & = & (& -3 & , & 1 & , & 1 &) \\
\lambda^{15} & = & (& 1 & , & 4 & , & 3 &) \\
\lambda^{16} & = & (& 4 & , & 2 & , & -1 &) \\
\lambda^{17} & = & (& 2 & , & 0 & , & -4 &) \\
\lambda^{18} & = & (& 0 & , & -1 & , & -2 &)
\end{array}
$$

$\Rightarrow p.d.s.:$

$\{0, 1, 3, 8, 12, 18\}$

Pro vytvoření p.d.s. můžeme použít také mocniny λ, jejichž souřadnice (x_1, x_2, x_3) splňují rovnici přímky (v projektivním prostoru, jehož prvky jsou prvky z $GF(5^3)$):

$$ax_1 + bx_2 + cx_3 = 0.$$

Pro vytvoření p.d.s. můžeme použít také mocniny λ, jejichž souřadnice (x_1, x_2, x_3) splňují rovnici přímky (v projektivním prostoru, jehož prvky jsou prvky z $GF(5^3)$):

$$ax_1 + bx_2 + cx_3 = 0.$$

$x_1 = 0 \Rightarrow$

$$\{0, 1, 3, 8, 12, 18\}$$

Pro vytvoření p.d.s. můžeme použít také mocniny λ, jejichž souřadnice (x_1, x_2, x_3) splňují rovnici přímky (v projektivním prostoru, jehož prvky jsou prvky z $GF(5^3)$):

$$ax_1 + bx_2 + cx_3 = 0.$$

$x_1 = 0 \Rightarrow$

$$\{0, 1, 3, 8, 12, 18\}$$

$x_2 = 0 \Rightarrow$

$$\{0, 2, 7, 11, 17, 30\}$$

Zkouška:

Zkouška:

Vytvoříme všechny možné rozdíly prvků z p.d.s. $\{0, 1, 3, 8, 12, 18\}$.

Zkouška:

Vytvoříme všechny možné rozdíly prvků z p.d.s. $\{0, 1, 3, 8, 12, 18\}$.
Obdržíme čísla patřící do různých zbytkových tříd modulo
$5^2 + 5 + 1 = 31$:

Zkouška:

Vytvoříme všechny možné rozdíly prvků z p.d.s. $\{0, 1, 3, 8, 12, 18\}$.
Obdržíme čísla patřící do různých zbytkových tříd modulo
$5^2 + 5 + 1 = 31$:

$-$	**0**	**1**	**3**	**8**	**12**	**18**
0	0	30	28	23	19	13
1	1	0	29	24	20	14
3	3	2	0	26	22	16
8	8	7	5	0	27	21
12	12	11	9	4	0	25
18	18	17	15	10	6	0

Př.:

Př.:

Vytvořte p.d.s. o $2^2 + 1$ prvcích.

Př.:

Vytvořte p.d.s. o $2^2 + 1$ prvcích.
Budeme potřebovat primitivní ireducibilní polynom třetího stupně nad $GF(2^2)$

Př.:

Vytvořte p.d.s. o $2^2 + 1$ prvcích.
Budeme potřebovat primitivní ireducibilní polynom třetího stupně nad $GF(2^2)$
Z tabulek (internet):

$$\alpha^{\mathbf{3}} + \alpha^{\mathbf{2}} + \alpha + (\mathbf{a} + \mathbf{1}),$$

Př.:

Vytvořte p.d.s. o $2^2 + 1$ prvcích.
Budeme potřebovat primitivní ireducibilní polynom třetího stupně nad $GF(2^2)$
Z tabulek (internet):

$$\alpha^{\mathbf{3}} + \alpha^{\mathbf{2}} + \alpha + (\mathbf{a} + \mathbf{1}),$$

kde a je kořenem ireducibilního polynomu $y^2 + y + 1 \in \mathbb{Z}_2[x]$

Př.:

Vytvořte p.d.s. o $2^2 + 1$ prvcích.
Budeme potřebovat primitivní ireducibilní polynom třetího stupně nad $GF(2^2)$
Z tabulek (internet):

$$\alpha^{\mathbf{3}} + \alpha^{\mathbf{2}} + \alpha + (\mathbf{a} + \mathbf{1}),$$

kde a je kořenem ireducibilního polynomu $y^2 + y + 1 \in \mathbb{Z}_2[x]$

Př.:

Vytvořte p.d.s. o $2^2 + 1$ prvcích.
Budeme potřebovat primitivní ireducibilní polynom třetího stupně nad $GF(2^2)$
Z tabulek (internet):

$$\alpha^{\mathbf{3}} + \alpha^{\mathbf{2}} + \alpha + (\mathbf{a} + \mathbf{1}),$$

kde a je kořenem ireducibilního polynomu $y^2 + y + 1 \in \mathbb{Z}_2[x]$
Obvykle značíme $x^2 + x + 1$

Př.:

Vytvořte p.d.s. o $2^2 + 1$ prvcích.
Budeme potřebovat primitivní ireducibilní polynom třetího stupně nad $GF(2^2)$
Z tabulek (internet):

$$\alpha^{\mathbf{3}} + \alpha^{\mathbf{2}} + \alpha + (\mathbf{a} + \mathbf{1}),$$

kde a je kořenem ireducibilního polynomu $y^2 + y + 1 \in \mathbb{Z}_2[x]$
Obvykle značíme $x^2 + x + 1$
$\Rightarrow$ vytvoříme $GF(2^2)$ jako $\mathbb{Z}_2[x]/_{[x^2+x+1]}$

Př.:

Vytvořte p.d.s. o $2^2 + 1$ prvcích.
Budeme potřebovat primitivní ireducibilní polynom třetího stupně nad $GF(2^2)$
Z tabulek (internet):

$$\alpha^{\mathbf{3}} + \alpha^{\mathbf{2}} + \alpha + (\mathbf{a} + \mathbf{1}),$$

kde a je kořenem ireducibilního polynomu $y^2 + y + 1 \in \mathbb{Z}_2[x]$
Obvykle značíme $x^2 + x + 1$
$\Rightarrow$ vytvoříme $GF(2^2)$ jako $\mathbb{Z}_2[x]/_{[x^2+x+1]}$ $\Rightarrow a = x$

Př.:

$\Rightarrow$ primitivní ireducibilní polynom třetího stupně nad $GF(2^2) = \mathbb{Z}_2[x]/_{[x^2+x+1]}$ je polynom:

Př.:

$\Rightarrow$ primitivní ireducibilní polynom třetího stupně nad $GF(2^2) = \mathbb{Z}_2[x]/_{[x^2+x+1]}$ je polynom:

$$\alpha^{\mathbf{3}} + \alpha^{\mathbf{2}} + \alpha + (\mathbf{x} + \mathbf{1}),$$

Př.:

$\Rightarrow$ primitivní ireducibilní polynom třetího stupně nad $GF(2^2) = \mathbb{Z}_2[x]/_{[x^2+x+1]}$ je polynom:

$$\alpha^{\mathbf{3}} + \alpha^{\mathbf{2}} + \alpha + (\mathbf{x} + \mathbf{1}),$$

Prvky z $GF(2^{3\cdot 2})$ potom můžeme chápat jako prvky ve tvaru

$$a\lambda^2 + b\lambda + c,$$

kde $a, b, c \in GF(2^2) = \mathbb{Z}_2[x]/_{[x^2+x+1]}$ a

Př.:

$\Rightarrow$ primitivní ireducibilní polynom třetího stupně nad $GF(2^2) = \mathbb{Z}_2[x]/_{[x^2+x+1]}$ je polynom:

$$\alpha^{\mathbf{3}} + \alpha^{\mathbf{2}} + \alpha + (\mathbf{x} + \mathbf{1}),$$

Prvky z $GF(2^{3\cdot 2})$ potom můžeme chápat jako prvky ve tvaru

$$a\lambda^2 + b\lambda + c,$$

kde $a, b, c \in GF(2^2) = \mathbb{Z}_2[x]/_{[x^2+x+1]}$ a λ splňuje podmínku

$$\lambda^{\mathbf{3}} + \lambda^{\mathbf{2}} + \lambda + (\mathbf{x} + \mathbf{1}) = \mathbf{0} \in \mathbf{GF}(\mathbf{2^{3\cdot 2}})$$

Násobení a sčítání v $GF(2^2) = \mathbb{Z}_2[x]/_{[x^2+x+1]}$

$+$	$\mathbf{0}$	$\mathbf{1}$	$\mathbf{x}$	$\mathbf{x+1}$
$\mathbf{0}$	0	1	x	$x+1$
$\mathbf{1}$	1	0	$x+1$	x
$\mathbf{x}$	x	$x+1$	0	1
$\mathbf{x+1}$	$x+1$	x	1	0

$\cdot$	$\mathbf{0}$	$\mathbf{1}$	$\mathbf{x}$	$\mathbf{x+1}$
$\mathbf{0}$	0	0	0	0
$\mathbf{1}$	0	1	x	$x+1$
$\mathbf{x}$	0	x	$x+1$	1
$\mathbf{x+1}$	0	$x+1$	1	x

Určíme mocniny prvku $\lambda \in GF(2^{3 \cdot 2})$, kde

Určíme mocniny prvku $\lambda \in GF(2^{3\cdot 2})$, kde

$$\lambda^i = x_1\lambda^2 + x_2\lambda + x_3$$

Určíme mocniny prvku $\lambda \in GF(2^{3\cdot 2})$, kde

$$\lambda^i = x_1\lambda^2 + x_2\lambda + x_3$$

$$\lambda^{i+1} = \lambda(x_1\lambda^2 + x_2\lambda + x_3)$$

Určíme mocniny prvku $\lambda \in GF(2^{3\cdot 2})$, kde

$$\lambda^i = x_1\lambda^2 + x_2\lambda + x_3$$

$$\begin{aligned} \lambda^{i+1} &= \lambda(x_1\lambda^2 + x_2\lambda + x_3) \\ \lambda^{i+1} &= x_1\lambda^3 + x_2\lambda^2 + x_3\lambda \end{aligned}$$

Určíme mocniny prvku $\lambda \in GF(2^{3\cdot 2})$, kde

$$\lambda^i = x_1\lambda^2 + x_2\lambda + x_3$$

$$\begin{aligned}
\lambda^{i+1} &= \lambda(x_1\lambda^2 + x_2\lambda + x_3) \\
\lambda^{i+1} &= x_1\lambda^3 + x_2\lambda^2 + x_3\lambda - x_1 \underbrace{(\lambda^3 + \lambda^2 + \lambda + (x+1))}_{=0}
\end{aligned}$$

Určíme mocniny prvku $\lambda \in GF(2^{3\cdot 2})$, kde

$$\lambda^i = x_1\lambda^2 + x_2\lambda + x_3$$

$$\begin{aligned}
\lambda^{i+1} &= \lambda(x_1\lambda^2 + x_2\lambda + x_3) \\
\lambda^{i+1} &= x_1\lambda^3 + x_2\lambda^2 + x_3\lambda - x_1 \underbrace{(\lambda^3 + \lambda^2 + \lambda + (x+1))}_{=0} \\
\lambda^{i+1} &= (x_2 - x_1)\lambda^2 + (x_3 - x_1)\lambda - x_1(x+1)
\end{aligned}$$

Určíme mocniny prvku $\lambda \in GF(2^{3\cdot 2})$, kde

$$\lambda^i = x_1\lambda^2 + x_2\lambda + x_3$$

$$\begin{aligned}
\lambda^{i+1} &= \lambda(x_1\lambda^2 + x_2\lambda + x_3) \\
\lambda^{i+1} &= x_1\lambda^3 + x_2\lambda^2 + x_3\lambda - x_1 \underbrace{(\lambda^3 + \lambda^2 + \lambda + (x+1))}_{=0} \\
\lambda^{i+1} &= (x_2 - x_1)\lambda^2 + (x_3 - x_1)\lambda - x_1(x+1)
\end{aligned}$$

Určíme mocniny prvku $\lambda \in GF(2^{3\cdot 2})$, kde

$$\lambda^i = x_1\lambda^2 + x_2\lambda + x_3$$

$$\begin{aligned}
\lambda^{i+1} &= \lambda(x_1\lambda^2 + x_2\lambda + x_3) \\
\lambda^{i+1} &= x_1\lambda^3 + x_2\lambda^2 + x_3\lambda - x_1 \underbrace{(\lambda^3 + \lambda^2 + \lambda + (x+1))}_{=0} \\
\lambda^{i+1} &= (x_2 - x_1)\lambda^2 + (x_3 - x_1)\lambda - x_1(x+1)
\end{aligned}$$

Souřadnicový zápis:
$\lambda^i = (x_1, x_2, x_3) \Rightarrow$

Určíme mocniny prvku $\lambda \in GF(2^{3\cdot 2})$, kde

$$\lambda^i = x_1\lambda^2 + x_2\lambda + x_3$$

$$\begin{aligned}
\lambda^{i+1} &= \lambda(x_1\lambda^2 + x_2\lambda + x_3) \\
\lambda^{i+1} &= x_1\lambda^3 + x_2\lambda^2 + x_3\lambda - x_1 \underbrace{(\lambda^3 + \lambda^2 + \lambda + (x+1))}_{=0} \\
\lambda^{i+1} &= (x_2 - x_1)\lambda^2 + (x_3 - x_1)\lambda - x_1(x+1)
\end{aligned}$$

Souřadnicový zápis:

$\lambda^i = (x_1, x_2, x_3) \Rightarrow \lambda^{i+1} = (x_2 - x_1, x_3 - x_1, -x_1(x+1))$.

Mocniny prvku λ - určujeme, dokud nenajdeme $2^2 + 1$ mocnin, jejichž první souřadnice je rovna nule. Souřadnicový zápis:
$\lambda^i = (x_1, x_2, x_3) \Rightarrow \lambda^{i+1} = (x_2 - x_1, x_3 - x_1, -x_1(x + 1))$.

Mocniny prvku λ - určujeme, dokud nenajdeme $2^2 + 1$ mocnin, jejichž první souřadnice je rovna nule. Souřadnicový zápis:
$\lambda^i = (x_1, x_2, x_3) \Rightarrow \lambda^{i+1} = (x_2 - x_1, x_3 - x_1, -x_1(x+1))$.

$$\lambda^0 = (0 , 0 , 1)$$

Mocniny prvku λ - určujeme, dokud nenajdeme $2^2 + 1$ mocnin, jejichž první souřadnice je rovna nule. Souřadnicový zápis:
$\lambda^i = (x_1, x_2, x_3) \Rightarrow \lambda^{i+1} = (x_2 - x_1, x_3 - x_1, -x_1(x+1))$.

$$\begin{array}{lcccccc} \lambda^0 & = & (& 0 & , & 0 & , & 1 &) \\ \lambda^1 & = & (& 0 & , & 1 & , & 0 &) \end{array}$$

Mocniny prvku λ - určujeme, dokud nenajdeme $2^2 + 1$ mocnin, jejichž první souřadnice je rovna nule. Souřadnicový zápis:
$\lambda^i = (x_1, x_2, x_3) \Rightarrow \lambda^{i+1} = (x_2 - x_1, x_3 - x_1, -x_1(x+1))$.

$$
\begin{array}{lcccccccc}
\lambda^0 & = & (& 0 & , & 0 & , & 1 &) \\
\lambda^1 & = & (& 0 & , & 1 & , & 0 &) \\
\lambda^2 & = & (& 1 & , & 0 & , & 0 &)
\end{array}
$$

Mocniny prvku λ - určujeme, dokud nenajdeme $2^2 + 1$ mocnin, jejichž první souřadnice je rovna nule. Souřadnicový zápis:
$\lambda^i = (x_1, x_2, x_3) \Rightarrow \lambda^{i+1} = (x_2 - x_1, x_3 - x_1, -x_1(x+1))$.

$$
\begin{array}{lcccccccc}
\lambda^0 & = & (& 0 & , & 0 & , & 1 &) \\
\lambda^1 & = & (& 0 & , & 1 & , & 0 &) \\
\lambda^2 & = & (& 1 & , & 0 & , & 0 &) \\
\lambda^3 & = & (& 1 & , & 1 & , & x+1 &)
\end{array}
$$

Mocniny prvku λ - určujeme, dokud nenajdeme $2^2 + 1$ mocnin, jejichž první souřadnice je rovna nule. Souřadnicový zápis:
$\lambda^i = (x_1, x_2, x_3) \Rightarrow \lambda^{i+1} = (x_2 - x_1, x_3 - x_1, -x_1(x+1))$.

$$
\begin{array}{lcccccccc}
\lambda^0 & = & (& 0 & , & 0 & , & 1 &) \\
\lambda^1 & = & (& 0 & , & 1 & , & 0 &) \\
\lambda^2 & = & (& 1 & , & 0 & , & 0 &) \\
\lambda^3 & = & (& 1 & , & 1 & , & x+1 &) \\
\lambda^4 & = & (& 0 & , & x & , & x+1 &)
\end{array}
$$

Mocniny prvku λ - určujeme, dokud nenajdeme $2^2 + 1$ mocnin, jejichž první souřadnice je rovna nule. Souřadnicový zápis:
$\lambda^i = (x_1, x_2, x_3) \Rightarrow \lambda^{i+1} = (x_2 - x_1, x_3 - x_1, -x_1(x+1))$.

$$
\begin{array}{lcccccccc}
\lambda^0 & = & (& 0 & , & 0 & , & 1 &) \\
\lambda^1 & = & (& 0 & , & 1 & , & 0 &) \\
\lambda^2 & = & (& 1 & , & 0 & , & 0 &) \\
\lambda^3 & = & (& 1 & , & 1 & , & x+1 &) \\
\lambda^4 & = & (& 0 & , & x & , & x+1 &) \\
\lambda^5 & = & (& x & , & x+1 & , & 0 &)
\end{array}
$$

Mocniny prvku λ - určujeme, dokud nenajdeme $2^2 + 1$ mocnin, jejichž první souřadnice je rovna nule. Souřadnicový zápis:
$\lambda^i = (x_1, x_2, x_3) \Rightarrow \lambda^{i+1} = (x_2 - x_1, x_3 - x_1, -x_1(x+1))$.

$$
\begin{array}{lcccccccc}
\lambda^0 & = & (& 0 & , & 0 & , & 1 &) \\
\lambda^1 & = & (& 0 & , & 1 & , & 0 &) \\
\lambda^2 & = & (& 1 & , & 0 & , & 0 &) \\
\lambda^3 & = & (& 1 & , & 1 & , & x+1 &) \\
\lambda^4 & = & (& 0 & , & x & , & x+1 &) \\
\lambda^5 & = & (& x & , & x+1 & , & 0 &) \\
\lambda^6 & = & (& 1 & , & x & , & 1 &)
\end{array}
$$

Mocniny prvku λ - určujeme, dokud nenajdeme $2^2 + 1$ mocnin, jejichž první souřadnice je rovna nule. Souřadnicový zápis:
$\lambda^i = (x_1, x_2, x_3) \Rightarrow \lambda^{i+1} = (x_2 - x_1, x_3 - x_1, -x_1(x+1))$.

$$
\begin{array}{lcccccccc}
\lambda^0 & = & (& 0 & , & 0 & , & 1 &) \\
\lambda^1 & = & (& 0 & , & 1 & , & 0 &) \\
\lambda^2 & = & (& 1 & , & 0 & , & 0 &) \\
\lambda^3 & = & (& 1 & , & 1 & , & x+1 &) \\
\lambda^4 & = & (& 0 & , & x & , & x+1 &) \\
\lambda^5 & = & (& x & , & x+1 & , & 0 &) \\
\lambda^6 & = & (& 1 & , & x & , & 1 &) \\
\lambda^7 & = & (& x+1 & , & 0 & , & x+1 &)
\end{array}
$$

Mocniny prvku λ - určujeme, dokud nenajdeme $2^2 + 1$ mocnin, jejichž první souřadnice je rovna nule. Souřadnicový zápis:
$\lambda^i = (x_1, x_2, x_3) \Rightarrow \lambda^{i+1} = (x_2 - x_1, x_3 - x_1, -x_1(x+1))$.

$$
\begin{array}{lcccccccc}
\lambda^0 & = & (& 0 & , & 0 & , & 1 &) \\
\lambda^1 & = & (& 0 & , & 1 & , & 0 &) \\
\lambda^2 & = & (& 1 & , & 0 & , & 0 &) \\
\lambda^3 & = & (& 1 & , & 1 & , & x+1 &) \\
\lambda^4 & = & (& 0 & , & x & , & x+1 &) \\
\lambda^5 & = & (& x & , & x+1 & , & 0 &) \\
\lambda^6 & = & (& 1 & , & x & , & 1 &) \\
\lambda^7 & = & (& x+1 & , & 0 & , & x+1 &) \\
\lambda^8 & = & (& x+1 & , & 0 & , & x &)
\end{array}
$$

Mocniny prvku λ - určujeme, dokud nenajdeme $2^2 + 1$ mocnin, jejichž první souřadnice je rovna nule. Souřadnicový zápis:
$\lambda^i = (x_1, x_2, x_3) \Rightarrow \lambda^{i+1} = (x_2 - x_1, x_3 - x_1, -x_1(x+1))$.

$$
\begin{array}{lcccccc}
\lambda^0 & = & (& 0 & , & 0 & , & 1 &) \\
\lambda^1 & = & (& 0 & , & 1 & , & 0 &) \\
\lambda^2 & = & (& 1 & , & 0 & , & 0 &) \\
\lambda^3 & = & (& 1 & , & 1 & , & x+1 &) \\
\lambda^4 & = & (& 0 & , & x & , & x+1 &) \\
\lambda^5 & = & (& x & , & x+1 & , & 0 &) \\
\lambda^6 & = & (& 1 & , & x & , & 1 &) \\
\lambda^7 & = & (& x+1 & , & 0 & , & x+1 &) \\
\lambda^8 & = & (& x+1 & , & 0 & , & x &) \\
\lambda^9 & = & (& x+1 & , & 1 & , & x &)
\end{array}
$$

Mocniny prvku λ - určujeme, dokud nenajdeme $2^2 + 1$ mocnin, jejichž první souřadnice je rovna nule. Souřadnicový zápis:
$\lambda^i = (x_1, x_2, x_3) \Rightarrow \lambda^{i+1} = (x_2 - x_1, x_3 - x_1, -x_1(x+1))$.

$$
\begin{array}{lcccccc}
\lambda^0 & = & (& 0 & , & 0 & , & 1 &) \\
\lambda^1 & = & (& 0 & , & 1 & , & 0 &) \\
\lambda^2 & = & (& 1 & , & 0 & , & 0 &) \\
\lambda^3 & = & (& 1 & , & 1 & , & x+1 &) \\
\lambda^4 & = & (& 0 & , & x & , & x+1 &) \\
\lambda^5 & = & (& x & , & x+1 & , & 0 &) \\
\lambda^6 & = & (& 1 & , & x & , & 1 &) \\
\lambda^7 & = & (& x+1 & , & 0 & , & x+1 &) \\
\lambda^8 & = & (& x+1 & , & 0 & , & x &) \\
\lambda^9 & = & (& x+1 & , & 1 & , & x &) \\
\lambda^{10} & = & (& x & , & 1 & , & x &)
\end{array}
$$

Mocniny prvku λ - určujeme, dokud nenajdeme $2^2 + 1$ mocnin, jejichž první souřadnice je rovna nule. Souřadnicový zápis:
$\lambda^i = (x_1, x_2, x_3) \Rightarrow \lambda^{i+1} = (x_2 - x_1, x_3 - x_1, -x_1(x+1))$.

$$
\begin{array}{lcccccc}
\lambda^0 & = & (& 0 & , & 0 & , & 1 &) \\
\lambda^1 & = & (& 0 & , & 1 & , & 0 &) \\
\lambda^2 & = & (& 1 & , & 0 & , & 0 &) \\
\lambda^3 & = & (& 1 & , & 1 & , & x+1 &) \\
\lambda^4 & = & (& 0 & , & x & , & x+1 &) \\
\lambda^5 & = & (& x & , & x+1 & , & 0 &) \\
\lambda^6 & = & (& 1 & , & x & , & 1 &) \\
\lambda^7 & = & (& x+1 & , & 0 & , & x+1 &) \\
\lambda^8 & = & (& x+1 & , & 0 & , & x &) \\
\lambda^9 & = & (& x+1 & , & 1 & , & x &) \\
\lambda^{10} & = & (& x & , & 1 & , & x &) \\
\lambda^{11} & = & (& x+1 & , & 0 & , & 1 &)
\end{array}
$$

Mocniny prvku λ - určujeme, dokud nenajdeme $2^2 + 1$ mocnin, jejichž první souřadnice je rovna nule. Souřadnicový zápis:
$\lambda^i = (x_1, x_2, x_3) \Rightarrow \lambda^{i+1} = (x_2 - x_1, x_3 - x_1, -x_1(x+1))$.

$$
\begin{array}{lcccccc}
\lambda^0 & = & (& 0 & , & 0 & , & 1 &) \\
\lambda^1 & = & (& 0 & , & 1 & , & 0 &) \\
\lambda^2 & = & (& 1 & , & 0 & , & 0 &) \\
\lambda^3 & = & (& 1 & , & 1 & , & x+1 &) \\
\lambda^4 & = & (& 0 & , & x & , & x+1 &) \\
\lambda^5 & = & (& x & , & x+1 & , & 0 &) \\
\lambda^6 & = & (& 1 & , & x & , & 1 &) \\
\lambda^7 & = & (& x+1 & , & 0 & , & x+1 &) \\
\lambda^8 & = & (& x+1 & , & 0 & , & x &) \\
\lambda^9 & = & (& x+1 & , & 1 & , & x &) \\
\lambda^{10} & = & (& x & , & 1 & , & x &) \\
\lambda^{11} & = & (& x+1 & , & 0 & , & 1 &) \\
\lambda^{12} & = & (& x+1 & , & x & , & x &)
\end{array}
$$

Mocniny prvku λ - určujeme, dokud nenajdeme $2^2 + 1$ mocnin, jejichž první souřadnice je rovna nule. Souřadnicový zápis:
$\lambda^i = (x_1, x_2, x_3) \Rightarrow \lambda^{i+1} = (x_2 - x_1, x_3 - x_1, -x_1(x+1))$.

$$
\begin{array}{lcccccc}
\lambda^0 & = & (& 0 & , & 0 & , & 1 &) \\
\lambda^1 & = & (& 0 & , & 1 & , & 0 &) \\
\lambda^2 & = & (& 1 & , & 0 & , & 0 &) \\
\lambda^3 & = & (& 1 & , & 1 & , & x+1 &) \\
\lambda^4 & = & (& 0 & , & x & , & x+1 &) \\
\lambda^5 & = & (& x & , & x+1 & , & 0 &) \\
\lambda^6 & = & (& 1 & , & x & , & 1 &) \\
\lambda^7 & = & (& x+1 & , & 0 & , & x+1 &) \\
\lambda^8 & = & (& x+1 & , & 0 & , & x &) \\
\lambda^9 & = & (& x+1 & , & 1 & , & x &) \\
\lambda^{10} & = & (& x & , & 1 & , & x &) \\
\lambda^{11} & = & (& x+1 & , & 0 & , & 1 &) \\
\lambda^{12} & = & (& x+1 & , & x & , & x &) \\
\lambda^{13} & = & (& 1 & , & 1 & , & x &)
\end{array}
$$

Mocniny prvku λ - určujeme, dokud nenajdeme $2^2 + 1$ mocnin, jejichž první souřadnice je rovna nule. Souřadnicový zápis:
$\lambda^i = (x_1, x_2, x_3) \Rightarrow \lambda^{i+1} = (x_2 - x_1, x_3 - x_1, -x_1(x+1))$.

$$
\begin{array}{lcccccc}
\lambda^0 & = & (& 0 & , & 0 & , & 1 &) \\
\lambda^1 & = & (& 0 & , & 1 & , & 0 &) \\
\lambda^2 & = & (& 1 & , & 0 & , & 0 &) \\
\lambda^3 & = & (& 1 & , & 1 & , & x+1 &) \\
\lambda^4 & = & (& 0 & , & x & , & x+1 &) \\
\lambda^5 & = & (& x & , & x+1 & , & 0 &) \\
\lambda^6 & = & (& 1 & , & x & , & 1 &) \\
\lambda^7 & = & (& x+1 & , & 0 & , & x+1 &) \\
\lambda^8 & = & (& x+1 & , & 0 & , & x &) \\
\lambda^9 & = & (& x+1 & , & 1 & , & x &) \\
\lambda^{10} & = & (& x & , & 1 & , & x &) \\
\lambda^{11} & = & (& x+1 & , & 0 & , & 1 &) \\
\lambda^{12} & = & (& x+1 & , & x & , & x &) \\
\lambda^{13} & = & (& 1 & , & 1 & , & x &) \\
\lambda^{14} & = & (& 0 & , & x+1 & , & x+1 &)
\end{array}
$$

Mocniny prvku λ - určujeme, dokud nenajdeme $2^2 + 1$ mocnin, jejichž první souřadnice je rovna nule. Souřadnicový zápis:
$\lambda^i = (x_1, x_2, x_3) \Rightarrow \lambda^{i+1} = (x_2 - x_1, x_3 - x_1, -x_1(x+1))$.

$$
\begin{array}{lcccccc}
\lambda^0 & = & (& 0 & , & 0 & , & 1 &) \\
\lambda^1 & = & (& 0 & , & 1 & , & 0 &) \\
\lambda^2 & = & (& 1 & , & 0 & , & 0 &) \\
\lambda^3 & = & (& 1 & , & 1 & , & x+1 &) \\
\lambda^4 & = & (& 0 & , & x & , & x+1 &) \\
\lambda^5 & = & (& x & , & x+1 & , & 0 &) \\
\lambda^6 & = & (& 1 & , & x & , & 1 &) \\
\lambda^7 & = & (& x+1 & , & 0 & , & x+1 &) \\
\lambda^8 & = & (& x+1 & , & 0 & , & x &) \\
\lambda^9 & = & (& x+1 & , & 1 & , & x &) \\
\lambda^{10} & = & (& x & , & 1 & , & x &) \\
\lambda^{11} & = & (& x+1 & , & 0 & , & 1 &) \\
\lambda^{12} & = & (& x+1 & , & x & , & x &) \\
\lambda^{13} & = & (& 1 & , & 1 & , & x &) \\
\lambda^{14} & = & (& 0 & , & x+1 & , & x+1 &) \\
\lambda^{15} & = & (& x+1 & , & x+1 & , & 0 &)
\end{array}
$$

Mocniny prvku λ - určujeme, dokud nenajdeme $2^2 + 1$ mocnin, jejichž první souřadnice je rovna nule. Souřadnicový zápis:
$\lambda^i = (x_1, x_2, x_3) \Rightarrow \lambda^{i+1} = (x_2 - x_1, x_3 - x_1, -x_1(x+1))$.

$$
\begin{array}{lcccccc}
\lambda^0 & = & (& 0 & , & 0 & , & 1 &) \\
\lambda^1 & = & (& 0 & , & 1 & , & 0 &) \\
\lambda^2 & = & (& 1 & , & 0 & , & 0 &) \\
\lambda^3 & = & (& 1 & , & 1 & , & x+1 &) \\
\lambda^4 & = & (& 0 & , & x & , & x+1 &) \\
\lambda^5 & = & (& x & , & x+1 & , & 0 &) \\
\lambda^6 & = & (& 1 & , & x & , & 1 &) \\
\lambda^7 & = & (& x+1 & , & 0 & , & x+1 &) \\
\lambda^8 & = & (& x+1 & , & 0 & , & x &) \\
\lambda^9 & = & (& x+1 & , & 1 & , & x &) \\
\lambda^{10} & = & (& x & , & 1 & , & x &) \\
\lambda^{11} & = & (& x+1 & , & 0 & , & 1 &) \\
\lambda^{12} & = & (& x+1 & , & x & , & x &) \\
\lambda^{13} & = & (& 1 & , & 1 & , & x &) \\
\lambda^{14} & = & (& 0 & , & x+1 & , & x+1 &) \\
\lambda^{15} & = & (& x+1 & , & x+1 & , & 0 &) \\
\lambda^{16} & = & (& 0 & , & x+1 & , & x &)
\end{array}
$$

Mocniny prvku λ - určujeme, dokud nenajdeme $2^2 + 1$ mocnin, jejichž první souřadnice je rovna nule. Souřadnicový zápis: $\lambda^i = (x_1, x_2, x_3) \Rightarrow \lambda^{i+1} = (x_2 - x_1, x_3 - x_1, -x_1(x+1))$.

$$
\begin{array}{lcccccc}
\lambda^0 & = & (& 0 & , & 0 & , & 1 &) \\
\lambda^1 & = & (& 0 & , & 1 & , & 0 &) \\
\lambda^2 & = & (& 1 & , & 0 & , & 0 &) \\
\lambda^3 & = & (& 1 & , & 1 & , & x+1 &) \\
\lambda^4 & = & (& 0 & , & x & , & x+1 &) \\
\lambda^5 & = & (& x & , & x+1 & , & 0 &) \\
\lambda^6 & = & (& 1 & , & x & , & 1 &) \\
\lambda^7 & = & (& x+1 & , & 0 & , & x+1 &) \\
\lambda^8 & = & (& x+1 & , & 0 & , & x &) \\
\lambda^9 & = & (& x+1 & , & 1 & , & x &) \\
\lambda^{10} & = & (& x & , & 1 & , & x &) \\
\lambda^{11} & = & (& x+1 & , & 0 & , & 1 &) \\
\lambda^{12} & = & (& x+1 & , & x & , & x &) \\
\lambda^{13} & = & (& 1 & , & 1 & , & x &) \\
\lambda^{14} & = & (& 0 & , & x+1 & , & x+1 &) \\
\lambda^{15} & = & (& x+1 & , & x+1 & , & 0 &) \\
\lambda^{16} & = & (& 0 & , & x+1 & , & x &)
\end{array}
$$

Mocniny prvku λ - určujeme, dokud nenajdeme $2^2 + 1$ mocnin, jejichž první souřadnice je rovna nule. Souřadnicový zápis: $\lambda^i = (x_1, x_2, x_3) \Rightarrow \lambda^{i+1} = (x_2 - x_1, x_3 - x_1, -x_1(x+1))$.

$$
\begin{array}{lcccccc}
\lambda^0 & = & (& 0 & , & 0 & , & 1 &) \\
\lambda^1 & = & (& 0 & , & 1 & , & 0 &) \\
\lambda^2 & = & (& 1 & , & 0 & , & 0 &) \\
\lambda^3 & = & (& 1 & , & 1 & , & x+1 &) \\
\lambda^4 & = & (& 0 & , & x & , & x+1 &) \\
\lambda^5 & = & (& x & , & x+1 & , & 0 &) \\
\lambda^6 & = & (& 1 & , & x & , & 1 &) \\
\lambda^7 & = & (& x+1 & , & 0 & , & x+1 &) \\
\lambda^8 & = & (& x+1 & , & 0 & , & x &) \\
\lambda^9 & = & (& x+1 & , & 1 & , & x &) \\
\lambda^{10} & = & (& x & , & 1 & , & x &) \\
\lambda^{11} & = & (& x+1 & , & 0 & , & 1 &) \\
\lambda^{12} & = & (& x+1 & , & x & , & x &) \\
\lambda^{13} & = & (& 1 & , & 1 & , & x &) \\
\lambda^{14} & = & (& 0 & , & x+1 & , & x+1 &) \\
\lambda^{15} & = & (& x+1 & , & x+1 & , & 0 &) \\
\lambda^{16} & = & (& 0 & , & x+1 & , & x &)
\end{array}
$$

Mocniny prvku λ - určujeme, dokud nenajdeme $2^2 + 1$ mocnin, jejichž první souřadnice je rovna nule. Souřadnicový zápis:
$\lambda^i = (x_1, x_2, x_3) \Rightarrow \lambda^{i+1} = (x_2 - x_1, x_3 - x_1, -x_1(x+1))$.

$$
\begin{array}{lcccccc}
\lambda^0 & = & (& 0 & , & 0 & , & 1 &) \\
\lambda^1 & = & (& 0 & , & 1 & , & 0 &) \\
\lambda^2 & = & (& 1 & , & 0 & , & 0 &) \\
\lambda^3 & = & (& 1 & , & 1 & , & x+1 &) \\
\lambda^4 & = & (& 0 & , & x & , & x+1 &) \\
\lambda^5 & = & (& x & , & x+1 & , & 0 &) \\
\lambda^6 & = & (& 1 & , & x & , & 1 &) \\
\lambda^7 & = & (& x+1 & , & 0 & , & x+1 &) \\
\lambda^8 & = & (& x+1 & , & 0 & , & x &) \\
\lambda^9 & = & (& x+1 & , & 1 & , & x &) \\
\lambda^{10} & = & (& x & , & 1 & , & x &) \\
\lambda^{11} & = & (& x+1 & , & 0 & , & 1 &) \\
\lambda^{12} & = & (& x+1 & , & x & , & x &) \\
\lambda^{13} & = & (& 1 & , & 1 & , & x &) \\
\lambda^{14} & = & (& 0 & , & x+1 & , & x+1 &) \\
\lambda^{15} & = & (& x+1 & , & x+1 & , & 0 &) \\
\lambda^{16} & = & (& 0 & , & x+1 & , & x &)
\end{array}
$$

Mocniny prvku λ - určujeme, dokud nenajdeme $2^2 + 1$ mocnin, jejichž první souřadnice je rovna nule. Souřadnicový zápis:
$\lambda^i = (x_1, x_2, x_3) \Rightarrow \lambda^{i+1} = (x_2 - x_1, x_3 - x_1, -x_1(x+1))$.

$$
\begin{array}{lcccccc}
\lambda^{0} & = & (& 0 & , & 0 & , & 1 &) \\
\lambda^{1} & = & (& 0 & , & 1 & , & 0 &) \\
\lambda^{2} & = & (& 1 & , & 0 & , & 0 &) \\
\lambda^{3} & = & (& 1 & , & 1 & , & x+1 &) \\
\lambda^{4} & = & (& 0 & , & x & , & x+1 &) \\
\lambda^{5} & = & (& x & , & x+1 & , & 0 &) \\
\lambda^{6} & = & (& 1 & , & x & , & 1 &) \\
\lambda^{7} & = & (& x+1 & , & 0 & , & x+1 &) \\
\lambda^{8} & = & (& x+1 & , & 0 & , & x &) \\
\lambda^{9} & = & (& x+1 & , & 1 & , & x &) \\
\lambda^{10} & = & (& x & , & 1 & , & x &) \\
\lambda^{11} & = & (& x+1 & , & 0 & , & 1 &) \\
\lambda^{12} & = & (& x+1 & , & x & , & x &) \\
\lambda^{13} & = & (& 1 & , & 1 & , & x &) \\
\lambda^{14} & = & (& 0 & , & x+1 & , & x+1 &) \\
\lambda^{15} & = & (& x+1 & , & x+1 & , & 0 &) \\
\lambda^{16} & = & (& 0 & , & x+1 & , & x &)
\end{array}
$$

Mocniny prvku λ - určujeme, dokud nenajdeme $2^2 + 1$ mocnin, jejichž první souřadnice je rovna nule. Souřadnicový zápis:
$\lambda^i = (x_1, x_2, x_3) \Rightarrow \lambda^{i+1} = (x_2 - x_1, x_3 - x_1, -x_1(x+1))$.

$$
\begin{array}{lcccccc}
\lambda^{0} & = & (& 0 & , & 0 & , & 1 &) \\
\lambda^{1} & = & (& 0 & , & 1 & , & 0 &) \\
\lambda^{2} & = & (& 1 & , & 0 & , & 0 &) \\
\lambda^{3} & = & (& 1 & , & 1 & , & x+1 &) \\
\lambda^{4} & = & (& 0 & , & x & , & x+1 &) \\
\lambda^{5} & = & (& x & , & x+1 & , & 0 &) \\
\lambda^{6} & = & (& 1 & , & x & , & 1 &) \\
\lambda^{7} & = & (& x+1 & , & 0 & , & x+1 &) \\
\lambda^{8} & = & (& x+1 & , & 0 & , & x &) \\
\lambda^{9} & = & (& x+1 & , & 1 & , & x &) \\
\lambda^{10} & = & (& x & , & 1 & , & x &) \\
\lambda^{11} & = & (& x+1 & , & 0 & , & 1 &) \\
\lambda^{12} & = & (& x+1 & , & x & , & x &) \\
\lambda^{13} & = & (& 1 & , & 1 & , & x &) \\
\lambda^{14} & = & (& 0 & , & x+1 & , & x+1 &) \\
\lambda^{15} & = & (& x+1 & , & x+1 & , & 0 &) \\
\lambda^{16} & = & (& 0 & , & x+1 & , & x &)
\end{array}
$$

Mocniny prvku λ - určujeme, dokud nenajdeme $2^2 + 1$ mocnin, jejichž první souřadnice je rovna nule. Souřadnicový zápis:
$\lambda^i = (x_1, x_2, x_3) \Rightarrow \lambda^{i+1} = (x_2 - x_1, x_3 - x_1, -x_1(x+1))$.

$$
\begin{array}{lcccccc}
\lambda^0 & = & (& 0 & , & 0 & , & 1 &) \\
\lambda^1 & = & (& 0 & , & 1 & , & 0 &) \\
\lambda^2 & = & (& 1 & , & 0 & , & 0 &) \\
\lambda^3 & = & (& 1 & , & 1 & , & x+1 &) \\
\lambda^4 & = & (& 0 & , & x & , & x+1 &) \\
\lambda^5 & = & (& x & , & x+1 & , & 0 &) \\
\lambda^6 & = & (& 1 & , & x & , & 1 &) \\
\lambda^7 & = & (& x+1 & , & 0 & , & x+1 &) \\
\lambda^8 & = & (& x+1 & , & 0 & , & x &) \\
\lambda^9 & = & (& x+1 & , & 1 & , & x &) \\
\lambda^{10} & = & (& x & , & 1 & , & x &) \\
\lambda^{11} & = & (& x+1 & , & 0 & , & 1 &) \\
\lambda^{12} & = & (& x+1 & , & x & , & x &) \\
\lambda^{13} & = & (& 1 & , & 1 & , & x &) \\
\lambda^{14} & = & (& 0 & , & x+1 & , & x+1 &) \\
\lambda^{15} & = & (& x+1 & , & x+1 & , & 0 &) \\
\lambda^{16} & = & (& 0 & , & x+1 & , & x &)
\end{array}
$$

$\Rightarrow p.d.s.$:

$\{0, 1, 4, 14, 16\}$

Pro vytvoření p.d.s. můžeme použít také mocniny λ, jejichž souřadnice (x_1, x_2, x_3) splňují rovnici přímky (v projektivním prostoru, jehož prvky jsou prvky z $GF(5^3)$):

$$ax_1 + bx_2 + cx_3 = 0.$$

Pro vytvoření p.d.s. můžeme použít také mocniny λ, jejichž souřadnice (x_1, x_2, x_3) splňují rovnici přímky (v projektivním prostoru, jehož prvky jsou prvky z $GF(5^3)$):

$$ax_1 + bx_2 + cx_3 = 0.$$

$x_1 = 0 \Rightarrow$

$$\{0, 1, 4, 14, 16\}$$

Pro vytvoření p.d.s. můžeme použít také mocniny λ, jejichž souřadnice (x_1, x_2, x_3) splňují rovnici přímky (v projektivním prostoru, jehož prvky jsou prvky z $GF(5^3)$):

$$ax_1 + bx_2 + cx_3 = 0.$$

$x_1 = 0 \Rightarrow$

$$\{0, 1, 4, 14, 16\}$$

$x_2 = 0 \Rightarrow$

$$\{0, 2, 7, 8, 11\}$$