Cíl: Vytvořit množinu dokonalých rozdílů o $5^1 + 1$ prvcích.

1. **Primitivní ireducibilní polynom třetího stupně nad $GF(5^1) = \mathbb{Z}_5$:**

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

   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

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

2. **Tabulka sčítání a násobení v $GF(5^1) = \mathbb{Z}_5$:**

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

·	**0**	**1**	**2**	**3**	**4**
0					
1					
2					
3					
4					

3. **Předpokládejme, že $\lambda^i = x_1\lambda^2 + x_2\lambda + x_3$. Určete λ^{i+1}, víte-li, že $\lambda^3 + \lambda + 1 = 0$ (viz bod 1.)**

4. **Určete souřadnice mocnin lambdy:**

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

5. **Určete nějakou množinu dokonalých rozdílů o šesti prvcích.**

Cíl: Vytvořit množinu dokonalých rozdílů o $2^2 + 1$ prvcích.

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

   $$\alpha^3 + \alpha^2 + \alpha + (x + 1)$$

   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

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

2. **Tabulka sčítání a násobení v $GF(2^2) = \mathbb{Z}_2[x]/_{[x^2+x+1]}$:**

$+$	**0**	**1**	**x**	**x + 1**
0				
1				
x				
x + 1				

$\cdot$	**0**	**1**	**x**	**x + 1**
0				
1				
x				
x + 1				

3. **Předpokládejme, že $\lambda^i = x_1\lambda^2 + x_2\lambda + x_3$. Určete λ^{i+1}, víte-li, že $\lambda^3 + \lambda^2 + \lambda + (x + 1) = 0 \in GF(2^{3\cdot 2})$ (viz bod 1.)**

4. **Určete souřadnice mocnin lambdy:**

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

5. **Určete nějakou množinu dokonalých rozdílů o pěti prvcích.**