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

Tabulka násobení v $\mathbb{Z}_3[x]/_{[x^2+1]}$

$\cdot$	0	1	2	x	$x+1$	$x+2$	2x	$2x+1$	$2x+2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
2	0	2	1	$2x$	$2x+2$	$2x+1$	x	$x+2$	$x+1$
x	0	x	$2x$	2	$x+2$	$2x+2$	1	$x+1$	$2x+1$
$x+1$	0	$x+1$	$2x+2$	$x+2$	$2x$	1	$2x+1$	2	x
$x+2$	0	$x+2$	$2x+1$	$2x+2$	1	x	$x+1$	$2x$	2
2x	0	$2x$	x	1	$2x+1$	$x+1$	2	$2x+2$	$x+2$
$2x+1$	0	$2x+1$	$x+2$	$x+1$	2	$2x$	$2x+2$	x	1
$2x+2$	0	$2x+2$	$x+1$	$2x+1$	x	2	$x+2$	1	$2x$

Tabulka násobení v $\mathbb{Z}_3[x]/_{[x^2+x+2]}$

$\cdot$	0	1	2	$x+2$	x	$x+1$	$2x+1$	$2x+2$	2x
0	0	0	0	0	0	0	0	0	0
1	0	1	2	$x+2$	x	$x+1$	$2x+1$	$2x+2$	$2x$
2	0	2	1	$2x+1$	$2x$	$2x+2$	$x+2$	$x+1$	x
$x+2$	0	$x+2$	$2x+1$	2	$x+1$	$2x$	1	x	$2x+2$
x	0	x	$2x$	$x+1$	$2x+1$	1	$2x+2$	2	$x+2$
$x+1$	0	$x+1$	$2x+2$	$2x$	1	$x+2$	x	$2x+1$	2
$2x+1$	0	$2x+1$	$x+2$	1	$2x+2$	x	2	$2x$	$x+1$
$2x+2$	0	$2x+2$	$x+1$	x	2	$2x+1$	$2x$	$x+2$	1
2x	0	$2x$	x	$2x+2$	$x+2$	2	$x+1$	1	$2x+1$

Tabulka násobení v $\mathbb{Z}_3[x]/_{[x^2+1]}$

$\cdot$	0	1	2	x	$x+1$	$x+2$	2x	$2x+1$	$2x+2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
2	0	2	1	$2x$	$2x+2$	$2x+1$	x	$x+2$	$x+1$
x	0	x	$2x$	2	$x+2$	$2x+2$	1	$x+1$	$2x+1$
$x+1$	0	$x+1$	$2x+2$	$x+2$	$2x$	1	$2x+1$	2	x
$x+2$	0	$x+2$	$2x+1$	$2x+2$	1	x	$x+1$	$2x$	2
2x	0	$2x$	x	1	$2x+1$	$x+1$	2	$2x+2$	$x+2$
$2x+1$	0	$2x+1$	$x+2$	$x+1$	2	$2x$	$2x+2$	x	1
$2x+2$	0	$2x+2$	$x+1$	$2x+1$	x	2	$x+2$	1	$2x$

Tabulka násobení v $\mathbb{Z}_3[x]/_{[x^2+x+2]}$

$\cdot$	0	1	2	$x+2$	x	$x+1$	$2x+1$	$2x+2$	2x
0	0	0	0	0	0	0	0	0	0
1	0	1	2	$x+2$	x	$x+1$	$2x+1$	$2x+2$	$2x$
2	0	2	1	$2x+1$	$2x$	$2x+2$	$x+2$	$x+1$	x
$x+2$	0	$x+2$	$2x+1$	2	$x+1$	$2x$	1	x	$2x+2$
x	0	x	$2x$	$x+1$	$2x+1$	1	$2x+2$	2	$x+2$
$x+1$	0	$x+1$	$2x+2$	$2x$	1	$x+2$	x	$2x+1$	2
$2x+1$	0	$2x+1$	$x+2$	1	$2x+2$	x	2	$2x$	$x+1$
$2x+2$	0	$2x+2$	$x+1$	x	2	$2x+1$	$2x$	$x+2$	1
2x	0	$2x$	x	$2x+2$	$x+2$	2	$x+1$	1	$2x+1$

Tabulka násobení v $\mathbb{Z}_3[x]/_{[x^2+1]}$

·	0	1	2	x	x + 1	x + 2	2x	2x + 1	2x + 2
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
2	0	2	1	$2x$	$2x+2$	$2x+1$	x	$x+2$	$x+1$
x	0	x	$2x$	2	$x+2$	$2x+2$	1	$x+1$	$2x+1$
x + 1	0	$x+1$	$2x+2$	$x+2$	$2x$	1	$2x+1$	2	x
x + 2	0	$x+2$	$2x+1$	$2x+2$	1	x	$x+1$	$2x$	2
2x	0	$2x$	x	1	$2x+1$	$x+1$	2	$2x+2$	$x+2$
2x + 1	0	$2x+1$	$x+2$	$x+1$	2	$2x$	$2x+2$	x	1
2x + 2	0	$2x+2$	$x+1$	$2x+1$	x	2	$x+2$	1	$2x$

Tabulka násobení v $\mathbb{Z}_3[x]/_{[x^2+x+2]}$

·	0	1	2	x + 2	x	x + 1	2x + 1	2x + 2	2x
0	0	0	0	0	0	0	0	0	0
1	0	1	2	$x+2$	x	$x+1$	$2x+1$	$2x+2$	$2x$
2	0	2	1	$2x+1$	$2x$	$2x+2$	$x+2$	$x+1$	x
x + 2	0	$x+2$	$2x+1$	2	$x+1$	$2x$	1	x	$2x+2$
x	0	x	$2x$	$x+1$	$2x+1$	1	$2x+2$	2	$x+2$
x + 1	0	$x+1$	$2x+2$	$2x$	1	$x+2$	x	$2x+1$	2
2x + 1	0	$2x+1$	$x+2$	1	$2x+2$	x	2	$2x$	$x+1$
2x + 2	0	$2x+2$	$x+1$	x	2	$2x+1$	$2x$	$x+2$	1
2x	0	$2x$	x	$2x+2$	$x+2$	2	$x+1$	1	$2x+1$

Tabulka násobení v $\mathbb{Z}_3[x]/_{[x^2+1]}$

·	0	1	2	x	x + 1	x + 2	2x	2x + 1	2x + 2
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
2	0	2	1	$2x$	$2x+2$	$2x+1$	x	$x+2$	$x+1$
x	0	x	$2x$	2	$x+2$	$2x+2$	1	$x+1$	$2x+1$
x + 1	0	$x+1$	$2x+2$	$x+2$	$2x$	1	$2x+1$	2	x
x + 2	0	$x+2$	$2x+1$	$2x+2$	1	x	$x+1$	$2x$	2
2x	0	$2x$	x	1	$2x+1$	$x+1$	2	$2x+2$	$x+2$
2x + 1	0	$2x+1$	$x+2$	$x+1$	2	$2x$	$2x+2$	x	1
2x + 2	0	$2x+2$	$x+1$	$2x+1$	x	2	$x+2$	1	$2x$

Tabulka násobení v $\mathbb{Z}_3[x]/_{[x^2+x+2]}$

·	0	1	2	x + 2	x	x + 1	2x + 1	2x + 2	2x
0	0	0	0	0	0	0	0	0	0
1	0	1	2	$x+2$	x	$x+1$	$2x+1$	$2x+2$	$2x$
2	0	2	1	$2x+1$	$2x$	$2x+2$	$x+2$	$x+1$	x
x + 2	0	$x+2$	$2x+1$	2	$x+1$	$2x$	1	x	$2x+2$
x	0	x	$2x$	$x+1$	$2x+1$	1	$2x+2$	2	$x+2$
x + 1	0	$x+1$	$2x+2$	$2x$	1	$x+2$	x	$2x+1$	2
2x + 1	0	$2x+1$	$x+2$	1	$2x+2$	x	2	$2x$	$x+1$
2x + 2	0	$2x+2$	$x+1$	x	2	$2x+1$	$2x$	$x+2$	1
2x	0	$2x$	x	$2x+2$	$x+2$	2	$x+1$	1	$2x+1$

Tabulka násobení v $\mathbb{Z}_3[x]/_{[x^2+1]}$

$\cdot$	0	1	2	x	$x+1$	$x+2$	2x	$2x+1$	$2x+2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
2	0	2	1	$2x$	$2x+2$	$2x+1$	x	$x+2$	$x+1$
x	0	x	$2x$	2	$x+2$	$2x+2$	1	$x+1$	$2x+1$
$x+1$	0	$x+1$	$2x+2$	$x+2$	$2x$	1	$2x+1$	2	x
$x+2$	0	$x+2$	$2x+1$	$2x+2$	1	x	$x+1$	$2x$	2
2x	0	$2x$	x	1	$2x+1$	$x+1$	2	$2x+2$	$x+2$
$2x+1$	0	$2x+1$	$x+2$	$x+1$	2	$2x$	$2x+2$	x	1
$2x+2$	0	$2x+2$	$x+1$	$2x+1$	x	2	$x+2$	1	$2x$

Tabulka násobení v $\mathbb{Z}_3[x]/_{[x^2+x+2]}$

$\cdot$	0	1	2	$x+2$	x	$x+1$	$2x+1$	$2x+2$	2x
0	0	0	0	0	0	0	0	0	0
1	0	1	2	$x+2$	x	$x+1$	$2x+1$	$2x+2$	$2x$
2	0	2	1	$2x+1$	$2x$	$2x+2$	$x+2$	$x+1$	x
$x+2$	0	$x+2$	$2x+1$	2	$x+1$	$2x$	1	x	$2x+2$
x	0	x	$2x$	$x+1$	$2x+1$	1	$2x+2$	2	$x+2$
$x+1$	0	$x+1$	$2x+2$	$2x$	1	$x+2$	x	$2x+1$	2
$2x+1$	0	$2x+1$	$x+2$	1	$2x+2$	x	2	$2x$	$x+1$
$2x+2$	0	$2x+2$	$x+1$	x	2	$2x+1$	$2x$	$x+2$	1
2x	0	$2x$	x	$2x+2$	$x+2$	2	$x+1$	1	$2x+1$

Tabulka násobení v $\mathbb{Z}_3[x]/_{[x^2+1]}$

·	0	1	2	x	x + 1	x + 2	2x	2x + 1	2x + 2
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
2	0	2	1	$2x$	$2x+2$	$2x+1$	x	$x+2$	$x+1$
x	0	x	$2x$	2	$x+2$	$2x+2$	1	$x+1$	$2x+1$
x + 1	0	$x+1$	$2x+2$	$x+2$	$2x$	1	$2x+1$	2	x
x + 2	0	$x+2$	$2x+1$	$2x+2$	1	x	$x+1$	$2x$	2
2x	0	$2x$	x	1	$2x+1$	$x+1$	2	$2x+2$	$x+2$
2x + 1	0	$2x+1$	$x+2$	$x+1$	2	$2x$	$2x+2$	x	1
2x + 2	0	$2x+2$	$x+1$	$2x+1$	x	2	$x+2$	1	$2x$

Tabulka násobení v $\mathbb{Z}_3[x]/_{[x^2+x+2]}$

·	0	1	2	x + 2	x	x + 1	2x + 1	2x + 2	2x
0	0	0	0	0	0	0	0	0	0
1	0	1	2	$x+2$	x	$x+1$	$2x+1$	$2x+2$	$2x$
2	0	2	1	$2x+1$	$2x$	$2x+2$	$x+2$	$x+1$	x
x + 2	0	$x+2$	$2x+1$	2	$x+1$	$2x$	1	x	$2x+2$
x	0	x	$2x$	$x+1$	$2x+1$	1	$2x+2$	2	$x+2$
x + 1	0	$x+1$	$2x+2$	$2x$	1	$x+2$	x	$2x+1$	2
2x + 1	0	$2x+1$	$x+2$	1	$2x+2$	x	2	$2x$	$x+1$
2x + 2	0	$2x+2$	$x+1$	x	2	$2x+1$	$2x$	$x+2$	1
2x	0	$2x$	x	$2x+2$	$x+2$	2	$x+1$	1	$2x+1$

Tabulka násobení v $\mathbb{Z}_3[x]/_{[x^2+1]}$

·	0	1	2	x	x + 1	x + 2	2x	2x + 1	2x + 2
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
2	0	2	1	$2x$	$2x+2$	$2x+1$	x	$x+2$	$x+1$
x	0	x	$2x$	2	$x+2$	$2x+2$	1	$x+1$	$2x+1$
x + 1	0	$x+1$	$2x+2$	$x+2$	$2x$	1	$2x+1$	2	x
x + 2	0	$x+2$	$2x+1$	$2x+2$	1	x	$x+1$	$2x$	2
2x	0	$2x$	x	1	$2x+1$	$x+1$	2	$2x+2$	$x+2$
2x + 1	0	$2x+1$	$x+2$	$x+1$	2	$2x$	$2x+2$	x	1
2x + 2	0	$2x+2$	$x+1$	$2x+1$	x	2	$x+2$	1	$2x$

Tabulka násobení v $\mathbb{Z}_3[x]/_{[x^2+x+2]}$

·	0	1	2	x + 2	x	x + 1	2x + 1	2x + 2	2x
0	0	0	0	0	0	0	0	0	0
1	0	1	2	$x+2$	x	$x+1$	$2x+1$	$2x+2$	$2x$
2	0	2	1	$2x+1$	$2x$	$2x+2$	$x+2$	$x+1$	x
x + 2	0	$x+2$	$2x+1$	2	$x+1$	$2x$	1	x	$2x+2$
x	0	x	$2x$	$x+1$	$2x+1$	1	$2x+2$	2	$x+2$
x + 1	0	$x+1$	$2x+2$	$2x$	1	$x+2$	x	$2x+1$	2
2x + 1	0	$2x+1$	$x+2$	1	$2x+2$	x	2	$2x$	$x+1$
2x + 2	0	$2x+2$	$x+1$	x	2	$2x+1$	$2x$	$x+2$	1
2x	0	$2x$	x	$2x+2$	$x+2$	2	$x+1$	1	$2x+1$

Tabulka násobení v $\mathbb{Z}_3[x]/_{[x^2+1]}$

·	0	1	2	x	x + 1	x + 2	2x	2x + 1	2x + 2
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
2	0	2	1	$2x$	$2x+2$	$2x+1$	x	$x+2$	$x+1$
x	0	x	$2x$	2	$x+2$	$2x+2$	1	$x+1$	$2x+1$
x + 1	0	$x+1$	$2x+2$	$x+2$	$2x$	1	$2x+1$	2	x
x + 2	0	$x+2$	$2x+1$	$2x+2$	1	x	$x+1$	$2x$	2
2x	0	$2x$	x	1	$2x+1$	$x+1$	2	$2x+2$	$x+2$
2x + 1	0	$2x+1$	$x+2$	$x+1$	2	$2x$	$2x+2$	x	1
2x + 2	0	$2x+2$	$x+1$	$2x+1$	x	2	$x+2$	1	$2x$

Tabulka násobení v $\mathbb{Z}_3[x]/_{[x^2+x+2]}$

·	0	1	2	x + 2	x	x + 1	2x + 1	2x + 2	2x
0	0	0	0	0	0	0	0	0	0
1	0	1	2	$x+2$	x	$x+1$	$2x+1$	$2x+2$	$2x$
2	0	2	1	$2x+1$	$2x$	$2x+2$	$x+2$	$x+1$	x
x + 2	0	$x+2$	$2x+1$	2	$x+1$	$2x$	1	x	$2x+2$
x	0	x	$2x$	$x+1$	$2x+1$	1	$2x+2$	2	$x+2$
x + 1	0	$x+1$	$2x+2$	$2x$	1	$x+2$	x	$2x+1$	2
2x + 1	0	$2x+1$	$x+2$	1	$2x+2$	x	2	$2x$	$x+1$
2x + 2	0	$2x+2$	$x+1$	x	2	$2x+1$	$2x$	$x+2$	1
2x	0	$2x$	x	$2x+2$	$x+2$	2	$x+1$	1	$2x+1$

Tabulka násobení v $\mathbb{Z}_3[x]/_{[x^2+1]}$

$\cdot$	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
2	0	2	1	$2x$	$2x+2$	$2x+1$	x	$x+2$	$x+1$
x	0	x	$2x$	2	$x+2$	$2x+2$	1	$x+1$	$2x+1$
$x+1$	0	$x+1$	$2x+2$	$x+2$	$2x$	1	$2x+1$	2	x
$x+2$	0	$x+2$	$2x+1$	$2x+2$	1	x	$x+1$	$2x$	2
$2x$	0	$2x$	x	1	$2x+1$	$x+1$	2	$2x+2$	$x+2$
$2x+1$	0	$2x+1$	$x+2$	$x+1$	2	$2x$	$2x+2$	x	1
$2x+2$	0	$2x+2$	$x+1$	$2x+1$	x	2	$x+2$	1	$2x$

Tabulka násobení v $\mathbb{Z}_3[x]/_{[x^2+x+2]}$

$\cdot$	0	1	2	$x+2$	x	$x+1$	$2x+1$	$2x+2$	$2x$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	$x+2$	x	$x+1$	$2x+1$	$2x+2$	$2x$
2	0	2	1	$2x+1$	$2x$	$2x+2$	$x+2$	$x+1$	x
$x+2$	0	$x+2$	$2x+1$	2	$x+1$	$2x$	1	x	$2x+2$
x	0	x	$2x$	$x+1$	$2x+1$	1	$2x+2$	2	$x+2$
$x+1$	0	$x+1$	$2x+2$	$2x$	1	$x+2$	x	$2x+1$	2
$2x+1$	0	$2x+1$	$x+2$	1	$2x+2$	x	2	$2x$	$x+1$
$2x+2$	0	$2x+2$	$x+1$	x	2	$2x+1$	$2x$	$x+2$	1
$2x$	0	$2x$	x	$2x+2$	$x+2$	2	$x+1$	1	$2x+1$

Tabulka násobení v $\mathbb{Z}_3[x]/_{[x^2+1]}$

·	0	1	2	x	x + 1	x + 2	2x	2x + 1	2x + 2
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
2	0	2	1	$2x$	$2x+2$	$2x+1$	x	$x+2$	$x+1$
x	0	x	$2x$	2	$x+2$	$2x+2$	1	$x+1$	$2x+1$
x + 1	0	$x+1$	$2x+2$	$x+2$	$2x$	1	$2x+1$	2	x
x + 2	0	$x+2$	$2x+1$	$2x+2$	1	x	$x+1$	$2x$	2
2x	0	$2x$	x	1	$2x+1$	$x+1$	2	$2x+2$	$x+2$
2x + 1	0	$2x+1$	$x+2$	$x+1$	2	$2x$	$2x+2$	x	1
2x + 2	0	$2x+2$	$x+1$	$2x+1$	x	2	$x+2$	1	$2x$

Tabulka násobení v $\mathbb{Z}_3[x]/_{[x^2+x+2]}$

·	0	1	2	x + 2	x	x + 1	2x + 1	2x + 2	2x
0	0	0	0	0	0	0	0	0	0
1	0	1	2	$x+2$	x	$x+1$	$2x+1$	$2x+2$	$2x$
2	0	2	1	$2x+1$	$2x$	$2x+2$	$x+2$	$x+1$	x
x + 2	0	$x+2$	$2x+1$	2	$x+1$	$2x$	1	x	$2x+2$
x	0	x	$2x$	$x+1$	$2x+1$	1	$2x+2$	2	$x+2$
x + 1	0	$x+1$	$2x+2$	$2x$	1	$x+2$	x	$2x+1$	2
2x + 1	0	$2x+1$	$x+2$	1	$2x+2$	x	2	$2x$	$x+1$
2x + 2	0	$2x+2$	$x+1$	x	2	$2x+1$	$2x$	$x+2$	1
2x	0	$2x$	x	$2x+2$	$x+2$	2	$x+1$	1	$2x+1$

Tabulka násobení v $\mathbb{Z}_3[x]/_{[x^2+1]}$

·	0	1	2	x	x + 1	x + 2	2x	2x + 1	2x + 2
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
2	0	2	1	$2x$	$2x+2$	$2x+1$	x	$x+2$	$x+1$
x	0	x	$2x$	2	$x+2$	$2x+2$	1	$x+1$	$2x+1$
x + 1	0	$x+1$	$2x+2$	$x+2$	$2x$	1	$2x+1$	2	x
x + 2	0	$x+2$	$2x+1$	$2x+2$	1	x	$x+1$	$2x$	2
2x	0	$2x$	x	1	$2x+1$	$x+1$	2	$2x+2$	$x+2$
2x + 1	0	$2x+1$	$x+2$	$x+1$	2	$2x$	$2x+2$	x	1
2x + 2	0	$2x+2$	$x+1$	$2x+1$	x	2	$x+2$	1	$2x$

Tabulka násobení v $\mathbb{Z}_3[x]/_{[x^2+x+2]}$

·	0	1	2	x + 2	x	x + 1	2x + 1	2x + 2	2x
0	0	0	0	0	0	0	0	0	0
1	0	1	2	$x+2$	x	$x+1$	$2x+1$	$2x+2$	$2x$
2	0	2	1	$2x+1$	$2x$	$2x+2$	$x+2$	$x+1$	x
x + 2	0	$x+2$	$2x+1$	2	$x+1$	$2x$	1	x	$2x+2$
x	0	x	$2x$	$x+1$	$2x+1$	1	$2x+2$	2	$x+2$
x + 1	0	$x+1$	$2x+2$	$2x$	1	$x+2$	x	$2x+1$	2
2x + 1	0	$2x+1$	$x+2$	1	$2x+2$	x	2	$2x$	$x+1$
2x + 2	0	$2x+2$	$x+1$	x	2	$2x+1$	$2x$	$x+2$	1
2x	0	$2x$	x	$2x+2$	$x+2$	2	$x+1$	1	$2x+1$

Tabulka násobení v $\mathbb{Z}_3[x]/_{[x^2+1]}$

$\cdot$	0	1	2	x	$x+1$	$x+2$	2x	$2x+1$	$2x+2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
2	0	2	1	$2x$	$2x+2$	$2x+1$	x	$x+2$	$x+1$
x	0	x	$2x$	2	$x+2$	$2x+2$	1	$x+1$	$2x+1$
$x+1$	0	$x+1$	$2x+2$	$x+2$	$2x$	1	$2x+1$	2	x
$x+2$	0	$x+2$	$2x+1$	$2x+2$	1	x	$x+1$	$2x$	2
2x	0	$2x$	x	1	$2x+1$	$x+1$	2	$2x+2$	$x+2$
$2x+1$	0	$2x+1$	$x+2$	$x+1$	2	$2x$	$2x+2$	x	1
$2x+2$	0	$2x+2$	$x+1$	$2x+1$	x	2	$x+2$	1	$2x$

Tabulka násobení v $\mathbb{Z}_3[x]/_{[x^2+x+2]}$

$\cdot$	0	1	2	$x+2$	x	$x+1$	$2x+1$	$2x+2$	2x
0	0	0	0	0	0	0	0	0	0
1	0	1	2	$x+2$	x	$x+1$	$2x+1$	$2x+2$	$2x$
2	0	2	1	$2x+1$	$2x$	$2x+2$	$x+2$	$x+1$	x
$x+2$	0	$x+2$	$2x+1$	2	$x+1$	$2x$	1	x	$2x+2$
x	0	x	$2x$	$x+1$	$2x+1$	1	$2x+2$	2	$x+2$
$x+1$	0	$x+1$	$2x+2$	$2x$	1	$x+2$	x	$2x+1$	2
$2x+1$	0	$2x+1$	$x+2$	1	$2x+2$	x	2	$2x$	$x+1$
$2x+2$	0	$2x+2$	$x+1$	x	2	$2x+1$	$2x$	$x+2$	1
2x	0	$2x$	x	$2x+2$	$x+2$	2	$x+1$	1	$2x+1$

Tabulka násobení v $\mathbb{Z}_3[x]/_{[x^2+1]}$

$\cdot$	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
2	0	2	1	$2x$	$2x+2$	$2x+1$	x	$x+2$	$x+1$
x	0	x	$2x$	2	$x+2$	$2x+2$	1	$x+1$	$2x+1$
$x+1$	0	$x+1$	$2x+2$	$x+2$	$2x$	1	$2x+1$	2	x
$x+2$	0	$x+2$	$2x+1$	$2x+2$	1	x	$x+1$	$2x$	2
$2x$	0	$2x$	x	1	$2x+1$	$x+1$	2	$2x+2$	$x+2$
$2x+1$	0	$2x+1$	$x+2$	$x+1$	2	$2x$	$2x+2$	x	1
$2x+2$	0	$2x+2$	$x+1$	$2x+1$	x	2	$x+2$	1	$2x$

Tabulka násobení v $\mathbb{Z}_3[x]/_{[x^2+x+2]}$

$\cdot$	0	1	2	$x+2$	x	$x+1$	$2x+1$	$2x+2$	$2x$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	$x+2$	x	$x+1$	$2x+1$	$2x+2$	$2x$
2	0	2	1	$2x+1$	$2x$	$2x+2$	$x+2$	$x+1$	x
$x+2$	0	$x+2$	$2x+1$	2	$x+1$	$2x$	1	x	$2x+2$
x	0	x	$2x$	$x+1$	$2x+1$	1	$2x+2$	2	$x+2$
$x+1$	0	$x+1$	$2x+2$	$2x$	1	$x+2$	x	$2x+1$	2
$2x+1$	0	$2x+1$	$x+2$	1	$2x+2$	x	2	$2x$	$x+1$
$2x+2$	0	$2x+2$	$x+1$	x	2	$2x+1$	$2x$	$x+2$	1
$2x$	0	$2x$	x	$2x+2$	$x+2$	2	$x+1$	1	$2x+1$

Tabulka násobení v $\mathbb{Z}_3[x]/_{[x^2+1]}$

$\cdot$	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
2	0	2	1	$2x$	$2x+2$	$2x+1$	x	$x+2$	$x+1$
x	0	x	$2x$	2	$x+2$	$2x+2$	1	$x+1$	$2x+1$
$x+1$	0	$x+1$	$2x+2$	$x+2$	$2x$	1	$2x+1$	2	x
$x+2$	0	$x+2$	$2x+1$	$2x+2$	1	x	$x+1$	$2x$	2
$2x$	0	$2x$	x	1	$2x+1$	$x+1$	2	$2x+2$	$x+2$
$2x+1$	0	$2x+1$	$x+2$	$x+1$	2	$2x$	$2x+2$	x	1
$2x+2$	0	$2x+2$	$x+1$	$2x+1$	x	2	$x+2$	1	$2x$

Tabulka násobení v $\mathbb{Z}_3[x]/_{[x^2+x+2]}$

$\cdot$	0	1	2	$x+2$	x	$x+1$	$2x+1$	$2x+2$	$2x$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	$x+2$	x	$x+1$	$2x+1$	$2x+2$	$2x$
2	0	2	1	$2x+1$	$2x$	$2x+2$	$x+2$	$x+1$	x
$x+2$	0	$x+2$	$2x+1$	2	$x+1$	$2x$	1	x	$2x+2$
x	0	x	$2x$	$x+1$	$2x+1$	1	$2x+2$	2	$x+2$
$x+1$	0	$x+1$	$2x+2$	$2x$	1	$x+2$	x	$2x+1$	2
$2x+1$	0	$2x+1$	$x+2$	1	$2x+2$	x	2	$2x$	$x+1$
$2x+2$	0	$2x+2$	$x+1$	x	2	$2x+1$	$2x$	$x+2$	1
$2x$	0	$2x$	x	$2x+2$	$x+2$	2	$x+1$	1	$2x+1$

Tabulka násobení v $\mathbb{Z}_3[x]/_{[x^2+1]}$

$\cdot$	0	1	2	x	$x+1$	$x+2$	2x	$2x+1$	$2x+2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
2	0	2	1	$2x$	$2x+2$	$2x+1$	x	$x+2$	$x+1$
x	0	x	$2x$	2	$x+2$	$2x+2$	1	$x+1$	$2x+1$
$x+1$	0	$x+1$	$2x+2$	$x+2$	$2x$	1	$2x+1$	2	x
$x+2$	0	$x+2$	$2x+1$	$2x+2$	1	x	$x+1$	$2x$	2
2x	0	$2x$	x	1	$2x+1$	$x+1$	2	$2x+2$	$x+2$
$2x+1$	0	$2x+1$	$x+2$	$x+1$	2	$2x$	$2x+2$	x	1
$2x+2$	0	$2x+2$	$x+1$	$2x+1$	x	2	$x+2$	1	$2x$

Tabulka násobení v $\mathbb{Z}_3[x]/_{[x^2+x+2]}$

$\cdot$	0	1	2	$x+2$	x	$x+1$	$2x+1$	$2x+2$	2x
0	0	0	0	0	0	0	0	0	0
1	0	1	2	$x+2$	x	$x+1$	$2x+1$	$2x+2$	$2x$
2	0	2	1	$2x+1$	$2x$	$2x+2$	$x+2$	$x+1$	x
$x+2$	0	$x+2$	$2x+1$	2	$x+1$	$2x$	1	x	$2x+2$
x	0	x	$2x$	$x+1$	$2x+1$	1	$2x+2$	2	$x+2$
$x+1$	0	$x+1$	$2x+2$	$2x$	1	$x+2$	x	$2x+1$	2
$2x+1$	0	$2x+1$	$x+2$	1	$2x+2$	x	2	$2x$	$x+1$
$2x+2$	0	$2x+2$	$x+1$	x	2	$2x+1$	$2x$	$x+2$	1
2x	0	$2x$	x	$2x+2$	$x+2$	2	$x+1$	1	$2x+1$

Tabulka násobení v $\mathbb{Z}_3[x]/_{[x^2+1]}$

·	0	1	2	x	x + 1	x + 2	2x	2x + 1	2x + 2
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
2	0	2	1	$2x$	$2x+2$	$2x+1$	x	$x+2$	$x+1$
x	0	x	$2x$	2	$x+2$	$2x+2$	1	$x+1$	$2x+1$
x + 1	0	$x+1$	$2x+2$	$x+2$	$2x$	1	$2x+1$	2	x
x + 2	0	$x+2$	$2x+1$	$2x+2$	1	x	$x+1$	$2x$	2
2x	0	$2x$	x	1	$2x+1$	$x+1$	2	$2x+2$	$x+2$
2x + 1	0	$2x+1$	$x+2$	$x+1$	2	$2x$	$2x+2$	x	1
2x + 2	0	$2x+2$	$x+1$	$2x+1$	x	2	$x+2$	1	$2x$

Tabulka násobení v $\mathbb{Z}_3[x]/_{[x^2+x+2]}$

·	0	1	2	x + 2	x	x + 1	2x + 1	2x + 2	2x
0	0	0	0	0	0	0	0	0	0
1	0	1	2	$x+2$	x	$x+1$	$2x+1$	$2x+2$	$2x$
2	0	2	1	$2x+1$	$2x$	$2x+2$	$x+2$	$x+1$	x
x + 2	0	$x+2$	$2x+1$	2	$x+1$	$2x$	1	x	$2x+2$
x	0	x	$2x$	$x+1$	$2x+1$	1	$2x+2$	2	$x+2$
x + 1	0	$x+1$	$2x+2$	$2x$	1	$x+2$	x	$2x+1$	2
2x + 1	0	$2x+1$	$x+2$	1	$2x+2$	x	2	$2x$	$x+1$
2x + 2	0	$2x+2$	$x+1$	x	2	$2x+1$	$2x$	$x+2$	1
2x	0	$2x$	x	$2x+2$	$x+2$	2	$x+1$	1	$2x+1$

Tabulka násobení v $\mathbb{Z}_3[x]/_{[x^2+1]}$

·	0	1	2	x	x + 1	x + 2	2x	2x + 1	2x + 2
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
2	0	2	1	$2x$	$2x+2$	$2x+1$	x	$x+2$	$x+1$
x	0	x	$2x$	2	$x+2$	$2x+2$	1	$x+1$	$2x+1$
x + 1	0	$x+1$	$2x+2$	$x+2$	$2x$	1	$2x+1$	2	x
x + 2	0	$x+2$	$2x+1$	$2x+2$	1	x	$x+1$	$2x$	2
2x	0	$2x$	x	1	$2x+1$	$x+1$	2	$2x+2$	$x+2$
2x + 1	0	$2x+1$	$x+2$	$x+1$	2	$2x$	$2x+2$	x	1
2x + 2	0	$2x+2$	$x+1$	$2x+1$	x	2	$x+2$	1	$2x$

Tabulka násobení v $\mathbb{Z}_3[x]/_{[x^2+x+2]}$

·	0	1	2	x + 2	x	x + 1	2x + 1	2x + 2	2x
0	0	0	0	0	0	0	0	0	0
1	0	1	2	$x+2$	x	$x+1$	$2x+1$	$2x+2$	$2x$
2	0	2	1	$2x+1$	$2x$	$2x+2$	$x+2$	$x+1$	x
x + 2	0	$x+2$	$2x+1$	2	$x+1$	$2x$	1	x	$2x+2$
x	0	x	$2x$	$x+1$	$2x+1$	1	$2x+2$	2	$x+2$
x + 1	0	$x+1$	$2x+2$	$2x$	1	$x+2$	x	$2x+1$	2
2x + 1	0	$2x+1$	$x+2$	1	$2x+2$	x	2	$2x$	$x+1$
2x + 2	0	$2x+2$	$x+1$	x	2	$2x+1$	$2x$	$x+2$	1
2x	0	$2x$	x	$2x+2$	$x+2$	2	$x+1$	1	$2x+1$

Isomorfismem $f : \mathbb{Z}_3[x]/_{[x^2+1]} \mapsto \mathbb{Z}_3[x]/_{[x^2+x+2]}$

Isomorfismem $f : \mathbb{Z}_3[x]/_{[x^2+1]} \mapsto \mathbb{Z}_3[x]/_{[x^2+x+2]}$ je zobrazení splňující pro každé $a, b \in \mathbb{Z}_3[x]/_{[x^2+1]}$ vztahy:

Isomorfismem $f : \mathbb{Z}_3[x]/_{[x^2+1]} \mapsto \mathbb{Z}_3[x]/_{[x^2+x+2]}$ je zobrazení splňující pro každé $a, b \in \mathbb{Z}_3[x]/_{[x^2+1]}$ vztahy:

$$f(a+b) \quad = \quad f(a) + f(b)$$

Isomorfismem $f : \mathbb{Z}_3[x]/_{[x^2+1]} \mapsto \mathbb{Z}_3[x]/_{[x^2+x+2]}$ je zobrazení splňující pro každé $a, b \in \mathbb{Z}_3[x]/_{[x^2+1]}$ vztahy:

$$f(a+b) = f(a)+f(b)$$

$$f(a \cdot b) = f(a) \cdot f(b)$$

Isomorfismem $f : \mathbb{Z}_3[x]/_{[x^2+1]} \mapsto \mathbb{Z}_3[x]/_{[x^2+x+2]}$ je zobrazení:

Isomorfismem $f : \mathbb{Z}_3[x]/_{[x^2+1]} \mapsto \mathbb{Z}_3[x]/_{[x^2+x+2]}$ je zobrazení:

$$\begin{array}{ccc} 0 & \rightarrow & 0 \end{array}$$

Isomorfismem $f : \mathbb{Z}_3[x]/_{[x^2+1]} \mapsto \mathbb{Z}_3[x]/_{[x^2+x+2]}$ je zobrazení:

$$\begin{array}{ccc} 0 & \rightarrow & 0 \\ 1 & \rightarrow & 1 \end{array}$$

Isomorfismem $f : \mathbb{Z}_3[x]/_{[x^2+1]} \mapsto \mathbb{Z}_3[x]/_{[x^2+x+2]}$ je zobrazení:

$$\begin{aligned} 0 &\to 0 \\ 1 &\to 1 \\ 2 &\to 2 \end{aligned}$$

Isomorfismem $f : \mathbb{Z}_3[x]/_{[x^2+1]} \mapsto \mathbb{Z}_3[x]/_{[x^2+x+2]}$ je zobrazení:

$$\begin{aligned} 0 &\rightarrow 0 \\ 1 &\rightarrow 1 \\ 2 &\rightarrow 2 \\ x &\rightarrow x+2 \end{aligned}$$

Isomorfismem $f : \mathbb{Z}_3[x]/_{[x^2+1]} \mapsto \mathbb{Z}_3[x]/_{[x^2+x+2]}$ je zobrazení:

$$\begin{aligned} 0 &\to 0 \\ 1 &\to 1 \\ 2 &\to 2 \\ x &\to x+2 \\ x+1 &\to x \end{aligned}$$

Isomorfismem $f : \mathbb{Z}_3[x]/_{[x^2+1]} \mapsto \mathbb{Z}_3[x]/_{[x^2+x+2]}$ je zobrazení:

$$\begin{aligned} 0 &\to 0 \\ 1 &\to 1 \\ 2 &\to 2 \\ x &\to x+2 \\ x+1 &\to x \\ x+2 &\to x+1 \end{aligned}$$

Isomorfismem $f : \mathbb{Z}_3[x]/_{[x^2+1]} \mapsto \mathbb{Z}_3[x]/_{[x^2+x+2]}$ je zobrazení:

$$\begin{aligned} 0 &\to 0 \\ 1 &\to 1 \\ 2 &\to 2 \\ x &\to x+2 \\ x+1 &\to x \\ x+2 &\to x+1 \\ 2x &\to 2x+1 \end{aligned}$$

Isomorfismem $f : \mathbb{Z}_3[x]/_{[x^2+1]} \mapsto \mathbb{Z}_3[x]/_{[x^2+x+2]}$ je zobrazení:

$$
\begin{aligned}
0 &\to 0 \\
1 &\to 1 \\
2 &\to 2 \\
x &\to x+2 \\
x+1 &\to x \\
x+2 &\to x+1 \\
2x &\to 2x+1 \\
2x+1 &\to 2x+2
\end{aligned}
$$

Isomorfismem $f : \mathbb{Z}_3[x]/_{[x^2+1]} \mapsto \mathbb{Z}_3[x]/_{[x^2+x+2]}$ je zobrazení:

$$
\begin{aligned}
0 &\to 0 \\
1 &\to 1 \\
2 &\to 2 \\
x &\to x+2 \\
x+1 &\to x \\
x+2 &\to x+1 \\
2x &\to 2x+1 \\
2x+1 &\to 2x+2 \\
2x+2 &\to 2x
\end{aligned}
$$

Isomorfismem $f : \mathbb{Z}_3[x]/_{[x^2+1]} \mapsto \mathbb{Z}_3[x]/_{[x^2+x+2]}$ je zobrazení:

$$\begin{aligned}
0 &\to 0 \\
1 &\to 1 \\
2 &\to 2 \\
x &\to x+2 \\
x+1 &\to x \\
x+2 &\to x+1 \\
2x &\to 2x+1 \\
2x+1 &\to 2x+2 \\
2x+2 &\to 2x
\end{aligned}$$

Není však jediným isomorfismem těchto těles!

Isomorfismem $f : \mathbb{Z}_3[x]/_{[x^2+1]} \mapsto \mathbb{Z}_3[x]/_{[x^2+x+2]}$ je zobrazení:

$$
\begin{aligned}
0 &\to 0 \\
1 &\to 1 \\
2 &\to 2 \\
x &\to x+2 \\
x+1 &\to x \\
x+2 &\to x+1 \\
2x &\to 2x+1 \\
2x+1 &\to 2x+2 \\
2x+2 &\to 2x
\end{aligned}
\qquad
0 \to 0
$$

Isomorfismem $f : \mathbb{Z}_3[x]/_{[x^2+1]} \mapsto \mathbb{Z}_3[x]/_{[x^2+x+2]}$ je zobrazení:

$$
\begin{aligned}
0 &\to 0 \\
1 &\to 1 \\
2 &\to 2 \\
x &\to x+2 \\
x+1 &\to x \\
x+2 &\to x+1 \\
2x &\to 2x+1 \\
2x+1 &\to 2x+2 \\
2x+2 &\to 2x
\end{aligned}
\qquad
\begin{aligned}
0 &\to 0 \\
1 &\to 1
\end{aligned}
$$

Isomorfismem $f : \mathbb{Z}_3[x]/_{[x^2+1]} \mapsto \mathbb{Z}_3[x]/_{[x^2+x+2]}$ je zobrazení:

$$
\begin{aligned}
0 &\to 0 \\
1 &\to 1 \\
2 &\to 2 \\
x &\to x+2 \\
x+1 &\to x \\
x+2 &\to x+1 \\
2x &\to 2x+1 \\
2x+1 &\to 2x+2 \\
2x+2 &\to 2x
\end{aligned}
\qquad
\begin{aligned}
0 &\to 0 \\
1 &\to 1 \\
2 &\to 2
\end{aligned}
$$

Isomorfismem $f : \mathbb{Z}_3[x]/_{[x^2+1]} \mapsto \mathbb{Z}_3[x]/_{[x^2+x+2]}$ je zobrazení:

$$
\begin{aligned}
0 &\to 0 \\
1 &\to 1 \\
2 &\to 2 \\
x &\to x+2 \\
x+1 &\to x \\
x+2 &\to x+1 \\
2x &\to 2x+1 \\
2x+1 &\to 2x+2 \\
2x+2 &\to 2x
\end{aligned}
\qquad
\begin{aligned}
0 &\to 0 \\
1 &\to 1 \\
2 &\to 2 \\
x &\to 2x+1
\end{aligned}
$$

Isomorfismem $f : \mathbb{Z}_3[x]/_{[x^2+1]} \mapsto \mathbb{Z}_3[x]/_{[x^2+x+2]}$ je zobrazení:

$$\begin{aligned} 0 &\to 0 \\ 1 &\to 1 \\ 2 &\to 2 \\ x &\to x+2 \\ x+1 &\to x \\ x+2 &\to x+1 \\ 2x &\to 2x+1 \\ 2x+1 &\to 2x+2 \\ 2x+2 &\to 2x \end{aligned}$$

$$\begin{aligned} 0 &\to 0 \\ 1 &\to 1 \\ 2 &\to 2 \\ x &\to 2x+1 \\ x+1 &\to 2x+2 \end{aligned}$$

Isomorfismem $f : \mathbb{Z}_3[x]/_{[x^2+1]} \mapsto \mathbb{Z}_3[x]/_{[x^2+x+2]}$ je zobrazení:

$$\begin{aligned} 0 &\to 0 \\ 1 &\to 1 \\ 2 &\to 2 \\ x &\to x+2 \\ x+1 &\to x \\ x+2 &\to x+1 \\ 2x &\to 2x+1 \\ 2x+1 &\to 2x+2 \\ 2x+2 &\to 2x \end{aligned}$$

$$\begin{aligned} 0 &\to 0 \\ 1 &\to 1 \\ 2 &\to 2 \\ x &\to 2x+1 \\ x+1 &\to 2x+2 \\ x+2 &\to 2x \end{aligned}$$

Isomorfismem $f : \mathbb{Z}_3[x]/_{[x^2+1]} \mapsto \mathbb{Z}_3[x]/_{[x^2+x+2]}$ je zobrazení:

$$
\begin{array}{rcl}
0 & \to & 0 \\
1 & \to & 1 \\
2 & \to & 2 \\
x & \to & x+2 \\
x+1 & \to & x \\
x+2 & \to & x+1 \\
2x & \to & 2x+1 \\
2x+1 & \to & 2x+2 \\
2x+2 & \to & 2x
\end{array}
\qquad
\begin{array}{rcl}
0 & \to & 0 \\
1 & \to & 1 \\
2 & \to & 2 \\
x & \to & 2x+1 \\
x+1 & \to & 2x+2 \\
x+2 & \to & 2x \\
2x & \to & x+2
\end{array}
$$

Isomorfismem $f : \mathbb{Z}_3[x]/_{[x^2+1]} \mapsto \mathbb{Z}_3[x]/_{[x^2+x+2]}$ je zobrazení:

$$
\begin{array}{rcl}
0 & \to & 0 \\
1 & \to & 1 \\
2 & \to & 2 \\
x & \to & x+2 \\
x+1 & \to & x \\
x+2 & \to & x+1 \\
2x & \to & 2x+1 \\
2x+1 & \to & 2x+2 \\
2x+2 & \to & 2x
\end{array}
\qquad
\begin{array}{rcl}
0 & \to & 0 \\
1 & \to & 1 \\
2 & \to & 2 \\
x & \to & 2x+1 \\
x+1 & \to & 2x+2 \\
x+2 & \to & 2x \\
2x & \to & x+2 \\
2x+1 & \to & x
\end{array}
$$

Isomorfismem $f : \mathbb{Z}_3[x]/_{[x^2+1]} \mapsto \mathbb{Z}_3[x]/_{[x^2+x+2]}$ je zobrazení:

$$
\begin{array}{rcl}
0 & \to & 0 \\
1 & \to & 1 \\
2 & \to & 2 \\
x & \to & x+2 \\
x+1 & \to & x \\
x+2 & \to & x+1 \\
2x & \to & 2x+1 \\
2x+1 & \to & 2x+2 \\
2x+2 & \to & 2x
\end{array}
\qquad
\begin{array}{rcl}
0 & \to & 0 \\
1 & \to & 1 \\
2 & \to & 2 \\
x & \to & 2x+1 \\
x+1 & \to & 2x+2 \\
x+2 & \to & 2x \\
2x & \to & x+2 \\
2x+1 & \to & x \\
2x+2 & \to & x+1
\end{array}
$$

Isomorfismem $f : \mathbb{Z}_3[x]/_{[x^2+1]} \mapsto \mathbb{Z}_3[x]/_{[x^2+x+2]}$ je zobrazení:

$$\begin{aligned} 0 &\to 0 \\ 1 &\to 1 \\ 2 &\to 2 \\ x &\to x+2 \\ x+1 &\to x \\ x+2 &\to x+1 \\ 2x &\to 2x+1 \\ 2x+1 &\to 2x+2 \\ 2x+2 &\to 2x \end{aligned} \qquad \begin{aligned} 0 &\to 0 \\ 1 &\to 1 \\ 2 &\to 2 \\ x &\to 2x+1 \\ x+1 &\to 2x+2 \\ x+2 &\to 2x \\ 2x &\to x+2 \\ 2x+1 &\to x \\ 2x+2 &\to x+1 \end{aligned}$$

Je také isomorfismem těchto těles!

Isomorfismem $f : \mathbb{Z}_3[x]/_{[x^2+1]} \mapsto \mathbb{Z}_3[x]/_{[x^2+x+2]}$ je zobrazení:

$$
\begin{array}{rcl}
0 & \to & 0 \\
1 & \to & 1 \\
2 & \to & 2 \\
x & \to & x+2 \\
x+1 & \to & x \\
x+2 & \to & x+1 \\
2x & \to & 2x+1 \\
2x+1 & \to & 2x+2 \\
2x+2 & \to & 2x
\end{array}
\qquad
\begin{array}{rcl}
0 & \to & 0 \\
1 & \to & 1 \\
2 & \to & 2 \\
x & \to & 2x+1 \\
x+1 & \to & 2x+2 \\
x+2 & \to & 2x \\
2x & \to & x+2 \\
2x+1 & \to & x \\
2x+2 & \to & x+1
\end{array}
$$

Jiný neexistuje!

Isomorfismem $f : \mathbb{Z}_3[x]/_{[x^2+1]} \mapsto \mathbb{Z}_3[x]/_{[x^2+x+2]}$ je zobrazení:

$$
\begin{array}{rcl}
0 & \to & 0 \\
1 & \to & 1 \\
2 & \to & 2 \\
x & \to & x+2 \\
x+1 & \to & x \\
x+2 & \to & x+1 \\
2x & \to & 2x+1 \\
2x+1 & \to & 2x+2 \\
2x+2 & \to & 2x
\end{array}
\qquad
\begin{array}{rcl}
0 & \to & 0 \\
1 & \to & 1 \\
2 & \to & 2 \\
x & \to & 2x+1 \\
x+1 & \to & 2x+2 \\
x+2 & \to & 2x \\
2x & \to & x+2 \\
2x+1 & \to & x \\
2x+2 & \to & x+1
\end{array}
$$

Proč?!

Shrnutí - Základní otázky a odpovědi

Shrnutí - Základní otázky a odpovědi

- **Existují konečná tělesa?**

Shrnutí - Základní otázky a odpovědi

- **Existují konečná tělesa?**

  Ano, například $(\mathbb{Z}_p, +, \cdot)$.

Shrnutí - Základní otázky a odpovědi

Shrnutí - Základní otázky a odpovědi

- **Kolik prvků mohou mít konečná tělesa?**

Shrnutí - Základní otázky a odpovědi

- **Kolik prvků mohou mít konečná tělesa?**

  Každé konečné těleso má p^n prvků, kde p je prvočíslo a n je přirozené číslo.

Shrnutí - Základní otázky a odpovědi

Shrnutí - Základní otázky a odpovědi

- **Existuje konečné těleso o p^n prvcích pro každé prvočíslo p a přirozené číslo n?**

Shrnutí - Základní otázky a odpovědi

- **Existuje konečné těleso o p^n prvcích pro každé prvočíslo p a přirozené číslo n?**

  Ano. Pro každé $n \in \mathbb{N}$, $n > 1$ a pro každé prvočíslo p existuje ireducibilní polynom $p(x) \in \mathbb{Z}_p[x]$, který je stupně n. Jsme tedy schopni zkonstruovat těleso $GF(p^n) = \mathbb{Z}_p[x]/p(x)$. Jde o těleso zbytků po dělení polynomem $p(x)$.

Shrnutí - Základní otázky a odpovědi

Shrnutí - Základní otázky a odpovědi

- **Proč by měl být polynom $p(x)$ použitý při konstrukci konečného tělesa ireducibilní?**

Shrnutí - Základní otázky a odpovědi

- **Proč by měl být polynom $p(x)$ použitý při konstrukci konečného tělesa ireducibilní?**

  V opačném případě by vzniklá struktura nebyla tělesem. Jednoduchý pčíklad. Pokud bychom se snažili sestrojit $GF(2^2)$ pomocí polynomu

  $$p(x) = x^2 - 1 = (x-1)(x+1) \in \mathbb{Z}_2,$$

  Došlo by k tomu, že

  $$\underbrace{((x-1)+[p(x)])}_{\neq \mathbf{0} = 0+[p]\in \mathbb{Z}_2[x]/_{[p(x)]}} \cdot \underbrace{((x+1)+[p(x)])}_{\neq \mathbf{0} = 0+[p]\in \mathbb{Z}_2[x]/_{[p(x)]}} = \underbrace{((x-1)(x+1)+[p(x)])}_{= \mathbf{0} = 0+[p]\in \mathbb{Z}_2[x]/_{[p(x)]}}$$

  A k tomu v tělese nesmí dojít! V tělese neexistují netriviální dělitelé nuly!

Shrnutí - Základní otázky a odpovědi

Shrnutí - Základní otázky a odpovědi

- **Ireducibilních polynomů stupně n nad $\mathbb{Z}_p[x]$ může být více. Dostanu pro různé ireducibilní polynomy při konstrukci konečného tělesa různá konečná tělesa?**

Shrnutí - Základní otázky a odpovědi

- **Ireducibilních polynomů stupně n nad $\mathbb{Z}_p[x]$ může být více. Dostanu pro různé ireducibilní polynomy při konstrukci konečného tělesa různá konečná tělesa?**

  Ano, i ne. Prvky těchto těles jsou stejné, tabulky sčítání také, tabulky násobení se však liší. Nicméně tato tělesa jsou izomorfní. To znamená, že při vhodném „přejmenování - označení“ prvků těles bychom obdrželi stejné tabulky násobení.

Shrnutí - Základní otázky a odpovědi

Shrnutí - Základní otázky a odpovědi

- **Je možné zkonstruovat konečné těleso i jiným, než výše uvedeným způsobem? Mohou býti prvky tělesa i něco jiného než zbytkové třídy modulo polynom?**

Shrnutí - Základní otázky a odpovědi

- **Je možné zkonstruovat konečné těleso i jiným, než výše uvedeným způsobem? Mohou býti prvky tělesa i něco jiného než zbytkové třídy modulo polynom?**

  Ale jistě, na množině prasátek {Norbert, Jeník, Dušan} definujme sčítání a násobení následovně:

Shrnutí - Základní otázky a odpovědi

- **Je možné zkonstruovat konečné těleso i jiným, než výše uvedeným způsobem? Mohou býti prvky tělesa i něco jiného než zbytkové třídy modulo polynom?**

  Ale jistě, na množině prasátek {Norbert, Jeník, Dušan} definujme sčítání a násobení následovně:

$+$	**N**	**J**	**D**
N	N	J	D
J	J	D	N
D	D	N	J

$\cdot$	**N**	**J**	**D**
N	N	N	N
J	N	J	D
D	N	D	J

Shrnutí - Základní otázky a odpovědi

- **Je možné zkonstruovat konečné těleso i jiným, než výše uvedeným způsobem? Mohou býti prvky tělesa i něco jiného než zbytkové třídy modulo polynom?**

  Ale jistě, na množině prasátek {Norbert, Jeník, Dušan} definujme sčítání a násobení následovně:

$+$	**N**	**J**	**D**
N	N	J	D
J	J	D	N
D	D	N	J

$\cdot$	**N**	**J**	**D**
N	N	N	N
J	N	J	D
D	N	D	J

  Toto těleso je však izomorfní s $\mathbb{Z}_3$. Obecně, libovolné konečné těleso je izomorfní s nějakým tělesem $(\mathbb{Z}_p[x]/_{[p(x)]}, +, \cdot)$.