Opakování: zbytkové třídy

Připomeňme, jak jsme definovali zbytkové třídy:

Definice. Nechť $m \in \mathbb{N}$. Pro libovolné $a \in \mathbb{Z}$ definujeme množinu $[a]_m = \{a + k \cdot m;\ k \in \mathbb{Z}\}$, kterou nazýváme zbytková třída modulo m obsahující a.

Opakování: zbytkové třídy

Připomeňme, jak jsme definovali zbytkové třídy:

Definice. Nechť $m \in \mathbb{N}$. Pro libovolné $a \in \mathbb{Z}$ definujeme množinu $[a]_m = \{a + k \cdot m;\ k \in \mathbb{Z}\}$, kterou nazýváme zbytková třída modulo m obsahující a.

Poznámka. Množina $[a]_m$ se skládá z právě těch celých čísel, která mají stejný zbytek po dělení číslem m jako číslo a.

Opakování: zbytkové třídy

Připomeňme, jak jsme definovali zbytkové třídy:

Definice. Nechť $m \in \mathbb{N}$. Pro libovolné $a \in \mathbb{Z}$ definujeme množinu $[a]_m = \{a + k \cdot m;\ k \in \mathbb{Z}\}$, kterou nazýváme zbytková třída modulo m obsahující a.

Poznámka. Množina $[a]_m$ se skládá z právě těch celých čísel, která mají stejný zbytek po dělení číslem m jako číslo a.

Věta. *Pro libovolná* $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$ *nastává* $[a]_m = [b]_m$ *právě tehdy, když* $m \mid a - b$, *tj. právě když* $a \equiv b \pmod{m}$.

Opakování: zbytkové třídy

Připomeňme, jak jsme definovali zbytkové třídy:

Definice. Nechť $m \in \mathbb{N}$. Pro libovolné $a \in \mathbb{Z}$ definujeme množinu $[a]_m = \{a + k \cdot m;\ k \in \mathbb{Z}\}$, kterou nazýváme zbytková třída modulo m obsahující a.

Poznámka. Množina $[a]_m$ se skládá z právě těch celých čísel, která mají stejný zbytek po dělení číslem m jako číslo a.

Věta. *Pro libovolná $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$ nastává $[a]_m = [b]_m$ právě tehdy, když $m \mid a - b$, tj. právě když $a \equiv b \pmod{m}$.*

Označení. Množinu všech zbytkových tříd modulo $m \in \mathbb{N}$ značíme $\mathbb{Z}_m$. Je tedy $\mathbb{Z}_m = \{[0]_m, [1]_m, [2]_m, \ldots, [m-1]_m\}$.

Opakování: zbytkové třídy

Připomeňme, jak jsme definovali zbytkové třídy:

Definice. Nechť $m \in \mathbb{N}$. Pro libovolné $a \in \mathbb{Z}$ definujeme množinu $[a]_m = \{a + k \cdot m;\ k \in \mathbb{Z}\}$, kterou nazýváme zbytková třída modulo m obsahující a.

Poznámka. Množina $[a]_m$ se skládá z právě těch celých čísel, která mají stejný zbytek po dělení číslem m jako číslo a.

Věta. *Pro libovolná $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$ nastává $[a]_m = [b]_m$ právě tehdy, když $m \mid a - b$, tj. právě když $a \equiv b \pmod{m}$.*

Označení. Množinu všech zbytkových tříd modulo $m \in \mathbb{N}$ značíme $\mathbb{Z}_m$. Je tedy $\mathbb{Z}_m = \{[0]_m, [1]_m, [2]_m, \ldots, [m-1]_m\}$.

Poznámka. Konstrukce množiny $\mathbb{Z}_m$ je speciální případ rozkladu grupy podle podgrupy. Je to rozklad grupy $(\mathbb{Z}, +)$ podle podgrupy $\{km; k \in \mathbb{Z}\}$ generované číslem m.

Opakování: operace na množině $\mathbb{Z}_m$

Připomeňme, jak jsme na množině $\mathbb{Z}_m$ zavedli operace pomocí reprezentantů, čímž jsme vytvořili okruh zbytkových tříd.

Opakování: operace na množině $\mathbb{Z}_m$

Připomeňme, jak jsme na množině $\mathbb{Z}_m$ zavedli operace pomocí reprezentantů, čímž jsme vytvořili okruh zbytkových tříd.
Potřebovali jsme přípravnou větu:

Opakování: operace na množině $\mathbb{Z}_m$

Připomeňme, jak jsme na množině $\mathbb{Z}_m$ zavedli operace pomocí reprezentantů, čímž jsme vytvořili okruh zbytkových tříd. Potřebovali jsme přípravnou větu:

Věta. *Nechť $m \in \mathbb{N}$, $a, b, c, d \in \mathbb{Z}$ jsou libovolná. Jestliže platí $[a]_m = [c]_m$, $[b]_m = [d]_m$, pak také*

$$[a + b]_m = [c + d]_m, \qquad [a \cdot b]_m = [c \cdot d]_m.$$

Opakování: operace na množině $\mathbb{Z}_m$

Připomeňme, jak jsme na množině $\mathbb{Z}_m$ zavedli operace pomocí reprezentantů, čímž jsme vytvořili okruh zbytkových tříd. Potřebovali jsme přípravnou větu:

Věta. *Nechť $m \in \mathbb{N}$, $a, b, c, d \in \mathbb{Z}$ jsou libovolná. Jestliže platí $[a]_m = [c]_m$, $[b]_m = [d]_m$, pak také*

$$[a + b]_m = [c + d]_m, \qquad [a \cdot b]_m = [c \cdot d]_m.$$

Důsledek. *Nechť $m \in \mathbb{N}$. Vztahy*

$$[a]_m + [b]_m = [a + b]_m,$$
$$[a]_m \cdot [b]_m = [a \cdot b]_m$$

pro libovolná $a, b \in \mathbb{Z}$ definují operace $+$ a $\cdot$ na množině $\mathbb{Z}_m$.

Opakování: operace na množině $\mathbb{Z}_m$

Připomeňme, jak jsme na množině $\mathbb{Z}_m$ zavedli operace pomocí reprezentantů, čímž jsme vytvořili okruh zbytkových tříd. Potřebovali jsme přípravnou větu:

Věta. *Nechť $m \in \mathbb{N}$, $a, b, c, d \in \mathbb{Z}$ jsou libovolná. Jestliže platí $[a]_m = [c]_m$, $[b]_m = [d]_m$, pak také*

$$[a + b]_m = [c + d]_m, \qquad [a \cdot b]_m = [c \cdot d]_m.$$

Důsledek. *Nechť $m \in \mathbb{N}$. Vztahy*

$$[a]_m + [b]_m = [a + b]_m,$$
$$[a]_m \cdot [b]_m = [a \cdot b]_m$$

pro libovolná $a, b \in \mathbb{Z}$ definují operace $+$ a $\cdot$ na množině $\mathbb{Z}_m$. Tato množina s těmito operacemi tvoří komutativní okruh $(\mathbb{Z}_m, +, \cdot)$.

Opakování: operace na množině $\mathbb{Z}_m$

Připomeňme, jak jsme na množině $\mathbb{Z}_m$ zavedli operace pomocí reprezentantů, čímž jsme vytvořili okruh zbytkových tříd. Potřebovali jsme přípravnou větu:

Věta. *Nechť $m \in \mathbb{N}$, $a, b, c, d \in \mathbb{Z}$ jsou libovolná. Jestliže platí $[a]_m = [c]_m$, $[b]_m = [d]_m$, pak také*

$$[a + b]_m = [c + d]_m, \qquad [a \cdot b]_m = [c \cdot d]_m.$$

Důsledek. *Nechť $m \in \mathbb{N}$. Vztahy*

$$[a]_m + [b]_m = [a + b]_m,$$
$$[a]_m \cdot [b]_m = [a \cdot b]_m$$

pro libovolná $a, b \in \mathbb{Z}$ definují operace $+$ a $\cdot$ na množině $\mathbb{Z}_m$. Tato množina s těmito operacemi tvoří komutativní okruh $(\mathbb{Z}_m, +, \cdot)$. Tento okruh je obor integrity, právě tehdy, když je tento okruh těleso, což nastává právě tehdy, když je m prvočíslo.

Zbytkové třídy polynomů nad tělesem

Definice. Nechť R je libovolné těleso. Zvolme pevně normovaný polynom $f \in R[x]$, $\mathrm{st}(f) \geq 1$.

Zbytkové třídy polynomů nad tělesem

Definice. Nechť R je libovolné těleso. Zvolme pevně normovaný polynom $f \in R[x]$, $\mathrm{st}(f) \geq 1$. Pro libovolný polynom $g \in R[x]$ definujeme množinu

$$[g]_f = \{g + k \cdot f;\ k \in R[x]\},$$

kterou nazveme zbytková třída okruhu polynomů $R[x]$ modulo f obsahující polynom g.

Zbytkové třídy polynomů nad tělesem

Definice. Nechť R je libovolné těleso. Zvolme pevně normovaný polynom $f \in R[x]$, $\mathrm{st}(f) \geq 1$. Pro libovolný polynom $g \in R[x]$ definujeme množinu

$$[g]_f = \{g + k \cdot f;\ k \in R[x]\},$$

kterou nazveme zbytková třída okruhu polynomů $R[x]$ modulo f obsahující polynom g.

Věta. *Nechť R je těleso a polynom $f \in R[x]$ je normovaný,* $\mathrm{st}(f) \geq 1$.

Zbytkové třídy polynomů nad tělesem

Definice. Nechť R je libovolné těleso. Zvolme pevně normovaný polynom $f \in R[x]$, $\mathrm{st}(f) \geq 1$. Pro libovolný polynom $g \in R[x]$ definujeme množinu

$$[g]_f = \{g + k \cdot f;\ k \in R[x]\},$$

kterou nazveme zbytková třída okruhu polynomů $R[x]$ modulo f obsahující polynom g.

Věta. *Nechť R je těleso a polynom $f \in R[x]$ je normovaný,* $\mathrm{st}(f) \geq 1$. *Množina $[0]_f$ obsahuje právě všechny polynomy z $R[x]$, které jsou dělitelné polynomem f.*

Zbytkové třídy polynomů nad tělesem

Definice. Nechť R je libovolné těleso. Zvolme pevně normovaný polynom $f \in R[x]$, $\mathrm{st}(f) \geq 1$. Pro libovolný polynom $g \in R[x]$ definujeme množinu

$$[g]_f = \{g + k \cdot f;\ k \in R[x]\},$$

kterou nazveme zbytková třída okruhu polynomů $R[x]$ modulo f obsahující polynom g.

Věta. *Nechť R je těleso a polynom $f \in R[x]$ je normovaný,* $\mathrm{st}(f) \geq 1$. *Množina $[0]_f$ obsahuje právě všechny polynomy z $R[x]$, které jsou dělitelné polynomem f. Platí, že $[0]_f$ je podgrupa grupy $(R[x], +)$ a že pro libovolný polynom $g \in R[x]$ je zbytková třída $[g]_f$ levá třída grupy $(R[x], +)$ podle podgrupy $[0]_f$.*

Zbytkové třídy polynomů nad tělesem

Definice. Nechť R je libovolné těleso. Zvolme pevně normovaný polynom $f \in R[x]$, $\mathrm{st}(f) \geq 1$. Pro libovolný polynom $g \in R[x]$ definujeme množinu

$$[g]_f = \{g + k \cdot f;\ k \in R[x]\},$$

kterou nazveme zbytková třída okruhu polynomů $R[x]$ modulo f obsahující polynom g.

Věta. *Nechť R je těleso a polynom $f \in R[x]$ je normovaný, $\mathrm{st}(f) \geq 1$. Množina $[0]_f$ obsahuje právě všechny polynomy z $R[x]$, které jsou dělitelné polynomem f. Platí, že $[0]_f$ je podgrupa grupy $(R[x], +)$ a že pro libovolný polynom $g \in R[x]$ je zbytková třída $[g]_f$ levá třída grupy $(R[x], +)$ podle podgrupy $[0]_f$.*

Poznámka. Pro libovolný polynom $g \in R[x]$ se množina $[g]_f$ skládá z právě těch polynomů ze $R[x]$, které mají stejný zbytek po dělení polynomem f jako polynom g.

Zbytkové třídy polynomů nad tělesem

Definice. Nechť R je libovolné těleso. Zvolme pevně normovaný polynom $f \in R[x]$, $\mathrm{st}(f) \geq 1$. Pro libovolný polynom $g \in R[x]$ definujeme množinu

$$[g]_f = \{g + k \cdot f;\ k \in R[x]\},$$

kterou nazveme zbytková třída okruhu polynomů $R[x]$ modulo f obsahující polynom g.

Věta. *Nechť R je těleso a polynom $f \in R[x]$ je normovaný,* $\mathrm{st}(f) \geq 1$. *Množina $[0]_f$ obsahuje právě všechny polynomy z $R[x]$, které jsou dělitelné polynomem f. Platí, že $[0]_f$ je podgrupa grupy $(R[x], +)$ a že pro libovolný polynom $g \in R[x]$ je zbytková třída $[g]_f$ levá třída grupy $(R[x], +)$ podle podgrupy $[0]_f$.*

Poznámka. Pro libovolný polynom $g \in R[x]$ se množina $[g]_f$ skládá z právě těch polynomů ze $R[x]$, které mají stejný zbytek po dělení polynomem f jako polynom g. Pro libovolné polynomy $g, h \in R[x]$ nastává $[g]_f = [h]_f$ právě tehdy, když $f \mid g - h$.

Množina zbytkových tříd polynomů

Označení. Nechť R je těleso a polynom $f \in R[x]$ je normovaný, $\mathrm{st}(f) \geq 1$.

Množina zbytkových tříd polynomů

Označení. Nechť R je těleso a polynom $f \in R[x]$ je normovaný, $\mathrm{st}(f) \geq 1$. Množinu všech zbytkových tříd okruhu polynomů $R[x]$ modulo f označme $R[x]/[0]_f$.

Množina zbytkových tříd polynomů

Označení. Nechť R je těleso a polynom $f \in R[x]$ je normovaný, $\mathrm{st}(f) \geq 1$. Množinu všech zbytkových tříd okruhu polynomů $R[x]$ modulo f označme $R[x]/[0]_f$. Je tedy

$$R[x]/[0]_f = \left\{[g]_f ; g \in R[x]\right\}.$$

Množina zbytkových tříd polynomů

Označení. Nechť R je těleso a polynom $f \in R[x]$ je normovaný, $\mathrm{st}(f) \geq 1$. Množinu všech zbytkových tříd okruhu polynomů $R[x]$ modulo f označme $R[x]/[0]_f$. Je tedy

$$R[x]/[0]_f = \left\{[g]_f; g \in R[x]\right\}.$$

Poznámka. Pro každou zbytkovou třídu platí, že společný zbytek jejích prvků po dělení polynomem f je také jejím prvkem, proto

$$R[x]/[0]_f = \left\{[g]_f; g \in R[x], \mathrm{st}(g) < \mathrm{st}(f)\right\}.$$

Množina zbytkových tříd polynomů

Označení. Nechť R je těleso a polynom $f \in R[x]$ je normovaný, $\mathrm{st}(f) \geq 1$. Množinu všech zbytkových tříd okruhu polynomů $R[x]$ modulo f označme $R[x]/[0]_f$. Je tedy

$$R[x]/[0]_f = \left\{[g]_f; g \in R[x]\right\}.$$

Poznámka. Pro každou zbytkovou třídu platí, že společný zbytek jejích prvků po dělení polynomem f je také jejím prvkem, proto

$$R[x]/[0]_f = \left\{[g]_f; g \in R[x], \mathrm{st}(g) < \mathrm{st}(f)\right\}.$$

Pro libovolné $g, h \in R[x]$, $\mathrm{st}(g) < \mathrm{st}(f)$, $\mathrm{st}(h) < \mathrm{st}(f)$, platí $[g]_f = [h]_f$, právě když $g = h$.

Množina zbytkových tříd polynomů

Označení. Nechť R je těleso a polynom $f \in R[x]$ je normovaný, $\mathrm{st}(f) \geq 1$. Množinu všech zbytkových tříd okruhu polynomů $R[x]$ modulo f označme $R[x]/[0]_f$. Je tedy

$$R[x]/[0]_f = \left\{[g]_f; g \in R[x]\right\}.$$

Poznámka. Pro každou zbytkovou třídu platí, že společný zbytek jejích prvků po dělení polynomem f je také jejím prvkem, proto

$$R[x]/[0]_f = \left\{[g]_f; g \in R[x], \mathrm{st}(g) < \mathrm{st}(f)\right\}.$$

Pro libovolné $g, h \in R[x]$, $\mathrm{st}(g) < \mathrm{st}(f)$, $\mathrm{st}(h) < \mathrm{st}(f)$, platí $[g]_f = [h]_f$, právě když $g = h$. Tedy každá zbytková třída $[g]_f$ obsahuje jediný polynom stupně menšího než $\mathrm{st}(f)$, totiž onen společný zbytek svých prvků po dělení polynomem f.

Množina zbytkových tříd polynomů

Označení. Nechť R je těleso a polynom $f \in R[x]$ je normovaný, $\mathrm{st}(f) \geq 1$. Množinu všech zbytkových tříd okruhu polynomů $R[x]$ modulo f označme $R[x]/[0]_f$. Je tedy

$$R[x]/[0]_f = \left\{[g]_f; g \in R[x]\right\}.$$

Poznámka. Pro každou zbytkovou třídu platí, že společný zbytek jejích prvků po dělení polynomem f je také jejím prvkem, proto

$$R[x]/[0]_f = \left\{[g]_f; g \in R[x], \mathrm{st}(g) < \mathrm{st}(f)\right\}.$$

Pro libovolné $g, h \in R[x]$, $\mathrm{st}(g) < \mathrm{st}(f)$, $\mathrm{st}(h) < \mathrm{st}(f)$, platí $[g]_f = [h]_f$, právě když $g = h$. Tedy každá zbytková třída $[g]_f$ obsahuje jediný polynom stupně menšího než $\mathrm{st}(f)$, totiž onen společný zbytek svých prvků po dělení polynomem f.

Příklad. Nechť p je prvočíslo a polynom $f \in \mathbb{Z}_p[x]$ je normovaný, $\mathrm{st}(f) \geq 1$.

Množina zbytkových tříd polynomů

Označení. Nechť R je těleso a polynom $f \in R[x]$ je normovaný, $\mathrm{st}(f) \geq 1$. Množinu všech zbytkových tříd okruhu polynomů $R[x]$ modulo f označme $R[x]/[0]_f$. Je tedy

$$R[x]/[0]_f = \left\{[g]_f; g \in R[x]\right\}.$$

Poznámka. Pro každou zbytkovou třídu platí, že společný zbytek jejích prvků po dělení polynomem f je také jejím prvkem, proto

$$R[x]/[0]_f = \left\{[g]_f; g \in R[x], \mathrm{st}(g) < \mathrm{st}(f)\right\}.$$

Pro libovolné $g, h \in R[x]$, $\mathrm{st}(g) < \mathrm{st}(f)$, $\mathrm{st}(h) < \mathrm{st}(f)$, platí $[g]_f = [h]_f$, právě když $g = h$. Tedy každá zbytková třída $[g]_f$ obsahuje jediný polynom stupně menšího než $\mathrm{st}(f)$, totiž onen společný zbytek svých prvků po dělení polynomem f.

Příklad. Nechť p je prvočíslo a polynom $f \in \mathbb{Z}_p[x]$ je normovaný, $\mathrm{st}(f) \geq 1$. Množina $\mathbb{Z}_p[x]/[0]_f$ má právě $p^{\mathrm{st}(f)}$ prvků.

Operace na množině zbytkových tříd polynomů

Věta. *Nechť R je těleso a polynom $f \in R[x]$ je normovaný,* $\mathrm{st}(f) \geq 1$.

Operace na množině zbytkových tříd polynomů

Věta. *Nechť R je těleso a polynom $f \in R[x]$ je normovaný,* $\mathrm{st}(f) \geq 1$. *Jestliže pro polynomy $g, h, r, s \in R[x]$ platí $[g]_f = [r]_f$, $[h]_f = [s]_f$, pak také platí $[g + h]_f = [r + s]_f$, $[g \cdot h]_f = [r \cdot s]_f$.*

Operace na množině zbytkových tříd polynomů

Věta. *Nechť R je těleso a polynom $f \in R[x]$ je normovaný,* $\mathrm{st}(f) \geq 1$. *Jestliže pro polynomy $g, h, r, s \in R[x]$ platí $[g]_f = [r]_f$, $[h]_f = [s]_f$, pak také platí $[g + h]_f = [r + s]_f$, $[g \cdot h]_f = [r \cdot s]_f$.*

Důkaz lze provést stejně jako pro zbytkové třídy celých čísel.

Operace na množině zbytkových tříd polynomů

Věta. *Nechť R je těleso a polynom $f \in R[x]$ je normovaný,* $\mathrm{st}(f) \geq 1$. *Jestliže pro polynomy $g, h, r, s \in R[x]$ platí $[g]_f = [r]_f$, $[h]_f = [s]_f$, pak také platí $[g + h]_f = [r + s]_f$, $[g \cdot h]_f = [r \cdot s]_f$.*

Důkaz lze provést stejně jako pro zbytkové třídy celých čísel.

Důsledek. *Nechť R je těleso a polynom $f \in R[x]$ je normovaný,* $\mathrm{st}(f) \geq 1$.

Operace na množině zbytkových tříd polynomů

Věta. *Nechť R je těleso a polynom $f \in R[x]$ je normovaný,* $\mathrm{st}(f) \geq 1$. *Jestliže pro polynomy $g, h, r, s \in R[x]$ platí $[g]_f = [r]_f$, $[h]_f = [s]_f$, pak také platí $[g+h]_f = [r+s]_f$, $[g \cdot h]_f = [r \cdot s]_f$.*

Důkaz lze provést stejně jako pro zbytkové třídy celých čísel.

Důsledek. *Nechť R je těleso a polynom $f \in R[x]$ je normovaný,* $\mathrm{st}(f) \geq 1$. *Vztahy*

$$[g]_f + [h]_f = [g+h]_f,$$
$$[g]_f \cdot [h]_f = [g \cdot h]_f$$

pro libovolné polynomy $g, h \in R[x]$ definují operace $+$ a $\cdot$ na množině $K = R[x]/[0]_f$.

Operace na množině zbytkových tříd polynomů

Věta. *Nechť R je těleso a polynom $f \in R[x]$ je normovaný,* $\mathrm{st}(f) \geq 1$. *Jestliže pro polynomy $g, h, r, s \in R[x]$ platí $[g]_f = [r]_f$, $[h]_f = [s]_f$, pak také platí $[g+h]_f = [r+s]_f$, $[g \cdot h]_f = [r \cdot s]_f$.*

Důkaz lze provést stejně jako pro zbytkové třídy celých čísel.

Důsledek. *Nechť R je těleso a polynom $f \in R[x]$ je normovaný,* $\mathrm{st}(f) \geq 1$. *Vztahy*

$$[g]_f + [h]_f = [g+h]_f,$$
$$[g]_f \cdot [h]_f = [g \cdot h]_f$$

pro libovolné polynomy $g, h \in R[x]$ definují operace $+$ a $\cdot$ na množině $K = R[x]/[0]_f$. Množina K s těmito operacemi tvoří netriviální komutativní okruh $(K, +, \cdot)$.

Operace na množině zbytkových tříd polynomů

Věta. *Nechť R je těleso a polynom $f \in R[x]$ je normovaný,* $\mathrm{st}(f) \geq 1$. *Jestliže pro polynomy $g, h, r, s \in R[x]$ platí $[g]_f = [r]_f$, $[h]_f = [s]_f$, pak také platí $[g+h]_f = [r+s]_f$, $[g \cdot h]_f = [r \cdot s]_f$.*

Důkaz lze provést stejně jako pro zbytkové třídy celých čísel.

Důsledek. *Nechť R je těleso a polynom $f \in R[x]$ je normovaný,* $\mathrm{st}(f) \geq 1$. *Vztahy*

$$[g]_f + [h]_f = [g+h]_f,$$
$$[g]_f \cdot [h]_f = [g \cdot h]_f$$

pro libovolné polynomy $g, h \in R[x]$ definují operace $+$ a $\cdot$ na množině $K = R[x]/[0]_f$. Množina K s těmito operacemi tvoří netriviální komutativní okruh $(K, +, \cdot)$. Okruh K je obor integrity právě tehdy, když je tento okruh těleso, což nastává právě tehdy, když f je ireducibilní polynom nad tělesem R.

Důkaz. Z předchozí věty plyne korektnost uvedených definic obou operací (tedy nezávislost výsledku operace na zvolených reprezentantech).

Důkaz. Z předchozí věty plyne korektnost uvedených definic obou operací (tedy nezávislost výsledku operace na zvolených reprezentantech). Každý z axiomů komutativního okruhu pro novou algebraickou strukturu $(K, +, \cdot)$ plyne z platnosti tohoto axiomu pro obor integrity $R[x]$,

Důkaz. Z předchozí věty plyne korektnost uvedených definic obou operací (tedy nezávislost výsledku operace na zvolených reprezentantech). Každý z axiomů komutativního okruhu pro novou algebraickou strukturu $(K, +, \cdot)$ plyne z platnosti tohoto axiomu pro obor integrity $R[x]$, ukažme si to například na komutativitě sčítání: pro libovolné polynomy $g, h \in R[x]$ platí

$$[g]_f + [h]_f = [g + h]_f = [h + g]_f = [h]_f + [g]_f.$$

Důkaz. Z předchozí věty plyne korektnost uvedených definic obou operací (tedy nezávislost výsledku operace na zvolených reprezentantech). Každý z axiomů komutativního okruhu pro novou algebraickou strukturu $(K, +, \cdot)$ plyne z platnosti tohoto axiomu pro obor integrity $R[x]$, ukažme si to například na komutativitě sčítání: pro libovolné polynomy $g, h \in R[x]$ platí

$$[g]_f + [h]_f = [g + h]_f = [h + g]_f = [h]_f + [g]_f .$$

Nulou (resp. jedničkou) v okruhu K je třída $[0]_f$ (resp. $[1]_f$) obsahující konstantní polynom 0 (resp. 1).

Důkaz. Z předchozí věty plyne korektnost uvedených definic obou operací (tedy nezávislost výsledku operace na zvolených reprezentantech). Každý z axiomů komutativního okruhu pro novou algebraickou strukturu $(K, +, \cdot)$ plyne z platnosti tohoto axiomu pro obor integrity $R[x]$, ukažme si to například na komutativitě sčítání: pro libovolné polynomy $g, h \in R[x]$ platí

$$[g]_f + [h]_f = [g + h]_f = [h + g]_f = [h]_f + [g]_f.$$

Nulou (resp. jedničkou) v okruhu K je třída $[0]_f$ (resp. $[1]_f$) obsahující konstantní polynom 0 (resp. 1).
Třída $[-g]_f$ je opačným prvkem ke třídě $[g]_f$.

Důkaz. Z předchozí věty plyne korektnost uvedených definic obou operací (tedy nezávislost výsledku operace na zvolených reprezentantech). Každý z axiomů komutativního okruhu pro novou algebraickou strukturu $(K, +, \cdot)$ plyne z platnosti tohoto axiomu pro obor integrity $R[x]$, ukažme si to například na komutativitě sčítání: pro libovolné polynomy $g, h \in R[x]$ platí

$$[g]_f + [h]_f = [g + h]_f = [h + g]_f = [h]_f + [g]_f.$$

Nulou (resp. jedničkou) v okruhu K je třída $[0]_f$ (resp. $[1]_f$) obsahující konstantní polynom 0 (resp. 1).
Třída $[-g]_f$ je opačným prvkem ke třídě $[g]_f$.
Je tedy K netriviální komutativní okruh.

Důkaz. Z předchozí věty plyne korektnost uvedených definic obou operací (tedy nezávislost výsledku operace na zvolených reprezentantech). Každý z axiomů komutativního okruhu pro novou algebraickou strukturu $(K, +, \cdot)$ plyne z platnosti tohoto axiomu pro obor integrity $R[x]$, ukažme si to například na komutativitě sčítání: pro libovolné polynomy $g, h \in R[x]$ platí

$$[g]_f + [h]_f = [g + h]_f = [h + g]_f = [h]_f + [g]_f.$$

Nulou (resp. jedničkou) v okruhu K je třída $[0]_f$ (resp. $[1]_f$) obsahující konstantní polynom 0 (resp. 1).
Třída $[-g]_f$ je opačným prvkem ke třídě $[g]_f$.
Je tedy K netriviální komutativní okruh. Dokažme ekvivalenci uvedených tří podmínek.

Důkaz. Z předchozí věty plyne korektnost uvedených definic obou operací (tedy nezávislost výsledku operace na zvolených reprezentantech). Každý z axiomů komutativního okruhu pro novou algebraickou strukturu $(K, +, \cdot)$ plyne z platnosti tohoto axiomu pro obor integrity $R[x]$, ukažme si to například na komutativitě sčítání: pro libovolné polynomy $g, h \in R[x]$ platí

$$[g]_f + [h]_f = [g + h]_f = [h + g]_f = [h]_f + [g]_f.$$

Nulou (resp. jedničkou) v okruhu K je třída $[0]_f$ (resp. $[1]_f$) obsahující konstantní polynom 0 (resp. 1).
Třída $[-g]_f$ je opačným prvkem ke třídě $[g]_f$.
Je tedy K netriviální komutativní okruh. Dokažme ekvivalenci uvedených tří podmínek.

1. Každé těleso je obor integrity, proto je-li K těleso, pak je K obor integrity.

2. Dokažme, že je-li K obor integrity, pak je polynom f ireducibilní nad R.

2. Dokažme, že je-li K obor integrity, pak je polynom f ireducibilní nad R. Předpokládejme, že polynom f není ireducibilní nad R, a tedy existují nekonstantní polynomy $r, s \in R[x]$ tak, že $r \cdot s = f$.

2. Dokažme, že je-li K obor integrity, pak je polynom f ireducibilní nad R. Předpokládejme, že polynom f není ireducibilní nad R, a tedy existují nekonstantní polynomy $r, s \in R[x]$ tak, že $r \cdot s = f$. Pak okruh K obsahuje dělitele nuly $[r]_f$, $[s]_f$, protože $\mathrm{st}(s) < \mathrm{st}(f)$, $\mathrm{st}(r) < \mathrm{st}(f)$, a tedy tyto prvky jsou nenulové, přitom $[r]_f \cdot [s]_f = [f]_f = [0]_f$, což je nula okruhu K.

2. Dokažme, že je-li K obor integrity, pak je polynom f ireducibilní nad R. Předpokládejme, že polynom f není ireducibilní nad R, a tedy existují nekonstantní polynomy $r, s \in R[x]$ tak, že $r \cdot s = f$. Pak okruh K obsahuje dělitele nuly $[r]_f$, $[s]_f$, protože $\mathrm{st}(s) < \mathrm{st}(f)$, $\mathrm{st}(r) < \mathrm{st}(f)$, a tedy tyto prvky jsou nenulové, přitom $[r]_f \cdot [s]_f = [f]_f = [0]_f$, což je nula okruhu K. Okruh K tedy není obor integrity.

2. Dokažme, že je-li K obor integrity, pak je polynom f ireducibilní nad R. Předpokládejme, že polynom f není ireducibilní nad R, a tedy existují nekonstantní polynomy $r, s \in R[x]$ tak, že $r \cdot s = f$. Pak okruh K obsahuje dělitele nuly $[r]_f$, $[s]_f$, protože $\mathrm{st}(s) < \mathrm{st}(f)$, $\mathrm{st}(r) < \mathrm{st}(f)$, a tedy tyto prvky jsou nenulové, přitom $[r]_f \cdot [s]_f = [f]_f = [0]_f$, což je nula okruhu K. Okruh K tedy není obor integrity.

3. Nechť je dále polynom f ireducibilní nad R.

2. Dokažme, že je-li K obor integrity, pak je polynom f ireducibilní nad R. Předpokládejme, že polynom f není ireducibilní nad R, a tedy existují nekonstantní polynomy $r, s \in R[x]$ tak, že $r \cdot s = f$. Pak okruh K obsahuje dělitele nuly $[r]_f$, $[s]_f$, protože $\mathrm{st}(s) < \mathrm{st}(f)$, $\mathrm{st}(r) < \mathrm{st}(f)$, a tedy tyto prvky jsou nenulové, přitom $[r]_f \cdot [s]_f = [f]_f = [0]_f$, což je nula okruhu K. Okruh K tedy není obor integrity.

3. Nechť je dále polynom f ireducibilní nad R. Libovolný nenulový prvek okruhu K je tvaru $[g]_f$, kde $g \neq 0$, $\mathrm{st}(g) < \mathrm{st}(f)$.

2. Dokažme, že je-li K obor integrity, pak je polynom f ireducibilní nad R. Předpokládejme, že polynom f není ireducibilní nad R, a tedy existují nekonstantní polynomy $r, s \in R[x]$ tak, že $r \cdot s = f$. Pak okruh K obsahuje dělitele nuly $[r]_f$, $[s]_f$, protože $\mathrm{st}(s) < \mathrm{st}(f)$, $\mathrm{st}(r) < \mathrm{st}(f)$, a tedy tyto prvky jsou nenulové, přitom $[r]_f \cdot [s]_f = [f]_f = [0]_f$, což je nula okruhu K. Okruh K tedy není obor integrity.

3. Nechť je dále polynom f ireducibilní nad R. Libovolný nenulový prvek okruhu K je tvaru $[g]_f$, kde $g \neq 0$, $\mathrm{st}(g) < \mathrm{st}(f)$. Z ireducibility polynomu $f(x)$ plyne $(g(x), f(x)) = 1$ a z Bezoutovy rovnosti dostáváme existenci polynomů $a, b \in R[x]$ takových, že $a \cdot g + b \cdot f = 1$.

2. Dokažme, že je-li K obor integrity, pak je polynom f ireducibilní nad R. Předpokládejme, že polynom f není ireducibilní nad R, a tedy existují nekonstantní polynomy $r, s \in R[x]$ tak, že $r \cdot s = f$. Pak okruh K obsahuje dělitele nuly $[r]_f$, $[s]_f$, protože $\mathrm{st}(s) < \mathrm{st}(f)$, $\mathrm{st}(r) < \mathrm{st}(f)$, a tedy tyto prvky jsou nenulové, přitom $[r]_f \cdot [s]_f = [f]_f = [0]_f$, což je nula okruhu K. Okruh K tedy není obor integrity.

3. Nechť je dále polynom f ireducibilní nad R. Libovolný nenulový prvek okruhu K je tvaru $[g]_f$, kde $g \neq 0$, $\mathrm{st}(g) < \mathrm{st}(f)$. Z ireducibility polynomu $f(x)$ plyne $(g(x), f(x)) = 1$ a z Bezoutovy rovnosti dostáváme existenci polynomů $a, b \in R[x]$ takových, že $a \cdot g + b \cdot f = 1$. Pak

$$[1]_f = [a \cdot g + b \cdot f]_f = [a \cdot g]_f = [a]_f \cdot [g]_f,$$

a tedy $[a]_f$ je inverzní prvek k prvku $[g]_f$.

2. Dokažme, že je-li K obor integrity, pak je polynom f ireducibilní nad R. Předpokládejme, že polynom f není ireducibilní nad R, a tedy existují nekonstantní polynomy $r, s \in R[x]$ tak, že $r \cdot s = f$. Pak okruh K obsahuje dělitele nuly $[r]_f$, $[s]_f$, protože $\mathrm{st}(s) < \mathrm{st}(f)$, $\mathrm{st}(r) < \mathrm{st}(f)$, a tedy tyto prvky jsou nenulové, přitom $[r]_f \cdot [s]_f = [f]_f = [0]_f$, což je nula okruhu K. Okruh K tedy není obor integrity.

3. Nechť je dále polynom f ireducibilní nad R. Libovolný nenulový prvek okruhu K je tvaru $[g]_f$, kde $g \neq 0$, $\mathrm{st}(g) < \mathrm{st}(f)$. Z ireducibility polynomu $f(x)$ plyne $(g(x), f(x)) = 1$ a z Bezoutovy rovnosti dostáváme existenci polynomů $a, b \in R[x]$ takových, že $a \cdot g + b \cdot f = 1$. Pak

$$[1]_f = [a \cdot g + b \cdot f]_f = [a \cdot g]_f = [a]_f \cdot [g]_f,$$

a tedy $[a]_f$ je inverzní prvek k prvku $[g]_f$. Dostali jsme, že K je těleso.

Příklad: čtyřprvkové těleso $\mathbb{Z}_2[x]/[0]_{x^2+x+1}$

Příklad. Zvolme $R = \mathbb{Z}_2$, $f = x^2 + x + 1 \in \mathbb{Z}_2[x]$.

Příklad: čtyřprvkové těleso $\mathbb{Z}_2[x]/[0]_{x^2+x+1}$

Příklad. Zvolme $R = \mathbb{Z}_2$, $f = x^2 + x + 1 \in \mathbb{Z}_2[x]$. Protože polynom f je ireducibilní nad $\mathbb{Z}_2$, dostáváme těleso

$$\mathbb{Z}_2[x]/[0]_{x^2+x+1} = \left\{[0]_{x^2+x+1}, [1]_{x^2+x+1}, [x]_{x^2+x+1}, [x+1]_{x^2+x+1}\right\}.$$

Příklad: čtyřprvkové těleso $\mathbb{Z}_2[x]/[0]_{x^2+x+1}$

Příklad. Zvolme $R = \mathbb{Z}_2$, $f = x^2 + x + 1 \in \mathbb{Z}_2[x]$. Protože polynom f je ireducibilní nad $\mathbb{Z}_2$, dostáváme těleso

$$\mathbb{Z}_2[x]/[0]_{x^2+x+1} = \left\{[0]_{x^2+x+1}, [1]_{x^2+x+1}, [x]_{x^2+x+1}, [x+1]_{x^2+x+1}\right\}.$$

Operace v tomto tělese počítáme pomocí reprezentantů, pokud při násobení reprezentantů dostaneme polynom příliš vysokého stupně, nahradíme jej zbytkem po dělení polynomem $x^2 + x + 1$,

Příklad: čtyřprvkové těleso $\mathbb{Z}_2[x]/[0]_{x^2+x+1}$

Příklad. Zvolme $R = \mathbb{Z}_2$, $f = x^2 + x + 1 \in \mathbb{Z}_2[x]$. Protože polynom f je ireducibilní nad $\mathbb{Z}_2$, dostáváme těleso

$$\mathbb{Z}_2[x]/[0]_{x^2+x+1} = \left\{[0]_{x^2+x+1}, [1]_{x^2+x+1}, [x]_{x^2+x+1}, [x+1]_{x^2+x+1}\right\}.$$

Operace v tomto tělese počítáme pomocí reprezentantů, pokud při násobení reprezentantů dostaneme polynom příliš vysokého stupně, nahradíme jej zbytkem po dělení polynomem $x^2 + x + 1$, například

$$\begin{aligned}
[x]_{x^2+x+1} + [x+1]_{x^2+x+1} &= [x + (x+1)]_{x^2+x+1} = [1]_{x^2+x+1}, \\
[x]_{x^2+x+1} \cdot [x+1]_{x^2+x+1} &= [x \cdot (x+1)]_{x^2+x+1} = \\
&= [x^2 + x]_{x^2+x+1} = [1]_{x^2+x+1},
\end{aligned}$$

kde poslední rovnost jsme dostali z toho, že zbytek po dělení polynomu $x^2 + x$ polynomem $x^2 + x + 1$ je 1.

Konečná tělesa

Z deváté přednášky víme, že multiplikativní grupa libovolného konečného tělesa je cyklická.

Konečná tělesa

Z deváté přednášky víme, že multiplikativní grupa libovolného konečného tělesa je cyklická. V navazujícím předmětu M3150 Algebra II jsou konečná tělesa jedním z důležitých témat.

Konečná tělesa

Z deváté přednášky víme, že multiplikativní grupa libovolného konečného tělesa je cyklická. V navazujícím předmětu M3150 Algebra II jsou konečná tělesa jedním z důležitých témat.
Bez důkazu si uveďme několik tvrzení, které tam budou dokázány:

Konečná tělesa

Z deváté přednášky víme, že multiplikativní grupa libovolného konečného tělesa je cyklická. V navazujícím předmětu M3150 Algebra II jsou konečná tělesa jedním z důležitých témat.
Bez důkazu si uveďme několik tvrzení, které tam budou dokázány:

Věta. Počet prvků libovolného konečného tělesa je mocnina jeho prvočíselné charakteristiky.

Konečná tělesa

Z deváté přednášky víme, že multiplikativní grupa libovolného konečného tělesa je cyklická. V navazujícím předmětu M3150 Algebra II jsou konečná tělesa jedním z důležitých témat.
Bez důkazu si uveďme několik tvrzení, které tam budou dokázány:

Věta. Počet prvků libovolného konečného tělesa je mocnina jeho prvočíselné charakteristiky.

Věta. Libovolná dvě konečná tělesa mající stejný počet prvků jsou izomorfní.

Konečná tělesa

Z deváté přednášky víme, že multiplikativní grupa libovolného konečného tělesa je cyklická. V navazujícím předmětu M3150 Algebra II jsou konečná tělesa jedním z důležitých témat.
Bez důkazu si uveďme několik tvrzení, které tam budou dokázány:

Věta. *Počet prvků libovolného konečného tělesa je mocnina jeho prvočíselné charakteristiky.*

Věta. *Libovolná dvě konečná tělesa mající stejný počet prvků jsou izomorfní.*

Věta. *Pro libovolné prvočíslo p a libovolné $m \in \mathbb{N}$ existuje normovaný ireducibilní polynom $f \in \mathbb{Z}_p[x]$, $\mathrm{st}(f) = m$.*

Konečná tělesa

Z deváté přednášky víme, že multiplikativní grupa libovolného konečného tělesa je cyklická. V navazujícím předmětu M3150 Algebra II jsou konečná tělesa jedním z důležitých témat.
Bez důkazu si uveďme několik tvrzení, které tam budou dokázány:

Věta. *Počet prvků libovolného konečného tělesa je mocnina jeho prvočíselné charakteristiky.*

Věta. *Libovolná dvě konečná tělesa mající stejný počet prvků jsou izomorfní.*

Věta. *Pro libovolné prvočíslo p a libovolné $m \in \mathbb{N}$ existuje normovaný ireducibilní polynom $f \in \mathbb{Z}_p[x]$, $\mathrm{st}(f) = m$.*

Důsledek. *Pro polynom f z předchozí věty je $K = \mathbb{Z}_p[x]/[0]_f$ těleso mající p^m prvků.*

Konečná tělesa

Z deváté přednášky víme, že multiplikativní grupa libovolného konečného tělesa je cyklická. V navazujícím předmětu M3150 Algebra II jsou konečná tělesa jedním z důležitých témat.
Bez důkazu si uveďme několik tvrzení, které tam budou dokázány:

Věta. *Počet prvků libovolného konečného tělesa je mocnina jeho prvočíselné charakteristiky.*

Věta. *Libovolná dvě konečná tělesa mající stejný počet prvků jsou izomorfní.*

Věta. *Pro libovolné prvočíslo p a libovolné $m \in \mathbb{N}$ existuje normovaný ireducibilní polynom $f \in \mathbb{Z}_p[x]$, $\mathrm{st}(f) = m$.*

Důsledek. *Pro polynom f z předchozí věty je $K = \mathbb{Z}_p[x]/[0]_f$ těleso mající p^m prvků. Polynom f je přitom možné zvolit tak, že prvek $[x]_f$ je generátor multiplikativní grupy $(K^\times, \cdot)$ tělesa K.*

Konečná tělesa

Z deváté přednášky víme, že multiplikativní grupa libovolného konečného tělesa je cyklická. V navazujícím předmětu M3150 Algebra II jsou konečná tělesa jedním z důležitých témat.
Bez důkazu si uveďme několik tvrzení, které tam budou dokázány:

Věta. *Počet prvků libovolného konečného tělesa je mocnina jeho prvočíselné charakteristiky.*

Věta. *Libovolná dvě konečná tělesa mající stejný počet prvků jsou izomorfní.*

Věta. *Pro libovolné prvočíslo p a libovolné $m \in \mathbb{N}$ existuje normovaný ireducibilní polynom $f \in \mathbb{Z}_p[x]$, $\mathrm{st}(f) = m$.*

Důsledek. *Pro polynom f z předchozí věty je $K = \mathbb{Z}_p[x]/[0]_f$ těleso mající p^m prvků. Polynom f je přitom možné zvolit tak, že prvek $[x]_f$ je generátor multiplikativní grupy $(K^\times, \cdot)$ tělesa K.*

Protože normovaných ireducibilních polynomů daného stupně m nad $\mathbb{Z}_p$ existuje jen konečně mnoho, je možné najít vhodný polynom metodou pokusů a omylů.

Jiný příklad: devítiprvkové těleso

Příklad. K sestrojení devítiprvkového tělesa potřebujeme normovaný ireducibilní kvadratický polynom $f(x) \in \mathbb{Z}_3[x]$.

Jiný příklad: devítiprvkové těleso

Příklad. K sestrojení devítiprvkového tělesa potřebujeme normovaný ireducibilní kvadratický polynom $f(x) \in \mathbb{Z}_3[x]$. Pro kvadratické (a kubické) polynomy platí, že jsou ireducibilní nad $\mathbb{Z}_3$, právě když nemají kořen v $\mathbb{Z}_3$.

Jiný příklad: devítiprvkové těleso

Příklad. K sestrojení devítiprvkového tělesa potřebujeme normovaný ireducibilní kvadratický polynom $f(x) \in \mathbb{Z}_3[x]$. Pro kvadratické (a kubické) polynomy platí, že jsou ireducibilní nad $\mathbb{Z}_3$, právě když nemají kořen v $\mathbb{Z}_3$. Snadno se ověří, že tuto podmínku splňuje polynom $x^2 + 1 \in \mathbb{Z}_3[x]$.

Jiný příklad: devítiprvkové těleso

Příklad. K sestrojení devítiprvkového tělesa potřebujeme normovaný ireducibilní kvadratický polynom $f(x) \in \mathbb{Z}_3[x]$. Pro kvadratické (a kubické) polynomy platí, že jsou ireducibilní nad $\mathbb{Z}_3$, právě když nemají kořen v $\mathbb{Z}_3$. Snadno se ověří, že tuto podmínku splňuje polynom $x^2 + 1 \in \mathbb{Z}_3[x]$. Zřejmě

$$\begin{aligned}\mathbb{Z}_3[x]/[0]_{x^2+1} = \{&[0]_{x^2+1}, [1]_{x^2+1}, [2]_{x^2+1}, [x]_{x^2+1}, [x+1]_{x^2+1},\\ &[x+2]_{x^2+1}, [2x]_{x^2+1}, [2x+1]_{x^2+1}, [2x+2]_{x^2+1}\}.\end{aligned}$$

Jiný příklad: devítiprvkové těleso

Příklad. K sestrojení devítiprvkového tělesa potřebujeme normovaný ireducibilní kvadratický polynom $f(x) \in \mathbb{Z}_3[x]$. Pro kvadratické (a kubické) polynomy platí, že jsou ireducibilní nad $\mathbb{Z}_3$, právě když nemají kořen v $\mathbb{Z}_3$. Snadno se ověří, že tuto podmínku splňuje polynom $x^2 + 1 \in \mathbb{Z}_3[x]$. Zřejmě

$$\begin{aligned}\mathbb{Z}_3[x]/[0]_{x^2+1} = \{&[0]_{x^2+1}, [1]_{x^2+1}, [2]_{x^2+1}, [x]_{x^2+1}, [x+1]_{x^2+1},\\ &[x+2]_{x^2+1}, [2x]_{x^2+1}, [2x+1]_{x^2+1}, [2x+2]_{x^2+1}\}.\end{aligned}$$

Ukažme si, že důkaz existence inverzního prvku na konci důkazu důsledku uvedeného na stranách 5-7 byl konstruktivní a dává nám užitečný algoritmus: spočítejme inverzní prvek k prvku $[2x+1]_{x^2+1}$.

Jiný příklad: devítiprvkové těleso

Příklad. K sestrojení devítiprvkového tělesa potřebujeme normovaný ireducibilní kvadratický polynom $f(x) \in \mathbb{Z}_3[x]$. Pro kvadratické (a kubické) polynomy platí, že jsou ireducibilní nad $\mathbb{Z}_3$, právě když nemají kořen v $\mathbb{Z}_3$. Snadno se ověří, že tuto podmínku splňuje polynom $x^2 + 1 \in \mathbb{Z}_3[x]$. Zřejmě

$$\begin{aligned}\mathbb{Z}_3[x]/[0]_{x^2+1} = \{&[0]_{x^2+1}, [1]_{x^2+1}, [2]_{x^2+1}, [x]_{x^2+1}, [x+1]_{x^2+1},\\ &[x+2]_{x^2+1}, [2x]_{x^2+1}, [2x+1]_{x^2+1}, [2x+2]_{x^2+1}\}.\end{aligned}$$

Ukažme si, že důkaz existence inverzního prvku na konci důkazu důsledku uvedeného na stranách 5-7 byl konstruktivní a dává nám užitečný algoritmus: spočítejme inverzní prvek k prvku $[2x+1]_{x^2+1}$. Pomocí Eukleidova algoritmu najdeme největší společný dělitel polynomů $x^2 + 1, 2x + 1 \in \mathbb{Z}_3[x]$, přestože víme, že jsou nesoudělné.

Jiný příklad: devítiprvkové těleso

Příklad. K sestrojení devítiprvkového tělesa potřebujeme normovaný ireducibilní kvadratický polynom $f(x) \in \mathbb{Z}_3[x]$. Pro kvadratické (a kubické) polynomy platí, že jsou ireducibilní nad $\mathbb{Z}_3$, právě když nemají kořen v $\mathbb{Z}_3$. Snadno se ověří, že tuto podmínku splňuje polynom $x^2 + 1 \in \mathbb{Z}_3[x]$. Zřejmě

$$\begin{aligned}\mathbb{Z}_3[x]/[0]_{x^2+1} =\{&[0]_{x^2+1}, [1]_{x^2+1}, [2]_{x^2+1}, [x]_{x^2+1}, [x+1]_{x^2+1},\\ &[x+2]_{x^2+1}, [2x]_{x^2+1}, [2x+1]_{x^2+1}, [2x+2]_{x^2+1}\}.\end{aligned}$$

Ukažme si, že důkaz existence inverzního prvku na konci důkazu důsledku uvedeného na stranách 5-7 byl konstruktivní a dává nám užitečný algoritmus: spočítejme inverzní prvek k prvku $[2x+1]_{x^2+1}$. Pomocí Eukleidova algoritmu najdeme největší společný dělitel polynomů $x^2 + 1, 2x + 1 \in \mathbb{Z}_3[x]$, přestože víme, že jsou nesoudělné. Ten najdeme v tomto případě jediným dělením:

$$x^2 + 1 = (2x + 1)(2x - 1) + 2.$$

Jiný příklad: devítiprvkové těleso

Příklad. K sestrojení devítiprvkového tělesa potřebujeme normovaný ireducibilní kvadratický polynom $f(x) \in \mathbb{Z}_3[x]$. Pro kvadratické (a kubické) polynomy platí, že jsou ireducibilní nad $\mathbb{Z}_3$, právě když nemají kořen v $\mathbb{Z}_3$. Snadno se ověří, že tuto podmínku splňuje polynom $x^2 + 1 \in \mathbb{Z}_3[x]$. Zřejmě

$$\begin{aligned}\mathbb{Z}_3[x]/[0]_{x^2+1} =\{&[0]_{x^2+1}, [1]_{x^2+1}, [2]_{x^2+1}, [x]_{x^2+1}, [x+1]_{x^2+1},\\ &[x+2]_{x^2+1}, [2x]_{x^2+1}, [2x+1]_{x^2+1}, [2x+2]_{x^2+1}\}.\end{aligned}$$

Ukažme si, že důkaz existence inverzního prvku na konci důkazu důsledku uvedeného na stranách 5-7 byl konstruktivní a dává nám užitečný algoritmus: spočítejme inverzní prvek k prvku $[2x+1]_{x^2+1}$. Pomocí Eukleidova algoritmu najdeme největší společný dělitel polynomů $x^2 + 1, 2x + 1 \in \mathbb{Z}_3[x]$, přestože víme, že jsou nesoudělné. Ten najdeme v tomto případě jediným dělením:

$$x^2 + 1 = (2x + 1)(2x - 1) + 2.$$

Bezoutova rovnost $1 = -(x^2 + 1) + (2x + 1)(2x - 1)$

Jiný příklad: devítiprvkové těleso

Příklad. K sestrojení devítiprvkového tělesa potřebujeme normovaný ireducibilní kvadratický polynom $f(x) \in \mathbb{Z}_3[x]$. Pro kvadratické (a kubické) polynomy platí, že jsou ireducibilní nad $\mathbb{Z}_3$, právě když nemají kořen v $\mathbb{Z}_3$. Snadno se ověří, že tuto podmínku splňuje polynom $x^2 + 1 \in \mathbb{Z}_3[x]$. Zřejmě

$$\begin{aligned}\mathbb{Z}_3[x]/[0]_{x^2+1} = \{&[0]_{x^2+1}, [1]_{x^2+1}, [2]_{x^2+1}, [x]_{x^2+1}, [x+1]_{x^2+1},\\ &[x+2]_{x^2+1}, [2x]_{x^2+1}, [2x+1]_{x^2+1}, [2x+2]_{x^2+1}\}.\end{aligned}$$

Ukažme si, že důkaz existence inverzního prvku na konci důkazu důsledku uvedeného na stranách 5-7 byl konstruktivní a dává nám užitečný algoritmus: spočítejme inverzní prvek k prvku $[2x+1]_{x^2+1}$. Pomocí Eukleidova algoritmu najdeme největší společný dělitel polynomů $x^2 + 1, 2x + 1 \in \mathbb{Z}_3[x]$, přestože víme, že jsou nesoudělné. Ten najdeme v tomto případě jediným dělením:

$$x^2 + 1 = (2x + 1)(2x - 1) + 2.$$

Bezoutova rovnost $1 = -(x^2 + 1) + (2x + 1)(2x - 1)$ pak dává $[2x + 1]^{-1}_{x^2+1} = [2x - 1]_{x^2+1}$.

Vnoření tělesa R do okruhu $R[x]/[0]_f$

Věta. *Nechť R je těleso a polynom $f \in R[x]$ je normovaný,* $\mathrm{st}(f) \geq 1$.

Vnoření tělesa R do okruhu $R[x]/[0]_f$

Věta. *Nechť R je těleso a polynom $f \in R[x]$ je normovaný,* $\mathrm{st}(f) \geq 1$. *Zobrazení $\varphi : R \to R[x]/[0]_f$ určené předpisem $\varphi(r) = [r]_f$ je injektivní homomorfismus okruhů.*

Vnoření tělesa R do okruhu $R[x]/[0]_f$

Věta. *Nechť R je těleso a polynom $f \in R[x]$ je normovaný,* $\mathrm{st}(f) \geq 1$. *Zobrazení $\varphi : R \to R[x]/[0]_f$ určené předpisem $\varphi(r) = [r]_f$ je injektivní homomorfismus okruhů.*

Poznámka. Díky předchozí větě můžeme ztotožnit libovolný prvek $r \in R$ s třídou $[r]_f$.

Vnoření tělesa R do okruhu $R[x]/[0]_f$

Věta. *Nechť R je těleso a polynom $f \in R[x]$ je normovaný,* $\mathrm{st}(f) \geq 1$. *Zobrazení $\varphi : R \to R[x]/[0]_f$ určené předpisem $\varphi(r) = [r]_f$ je injektivní homomorfismus okruhů.*

Poznámka. Díky předchozí větě můžeme ztotožnit libovolný prvek $r \in R$ s třídou $[r]_f$. Po tomto ztotožnění se R stane podokruhem okruhu $K = R[x]/[0]_f$.

Vnoření tělesa R do okruhu $R[x]/[0]_f$

Věta. *Nechť R je těleso a polynom $f \in R[x]$ je normovaný,* $\mathrm{st}(f) \geq 1$. *Zobrazení $\varphi : R \to R[x]/[0]_f$ určené předpisem $\varphi(r) = [r]_f$ je injektivní homomorfismus okruhů.*

Poznámka. Díky předchozí větě můžeme ztotožnit libovolný prvek $r \in R$ s třídou $[r]_f$. Po tomto ztotožnění se R stane podokruhem okruhu $K = R[x]/[0]_f$. Označme $\alpha = [x]_f$.

Vnoření tělesa R do okruhu $R[x]/[0]_f$

Věta. *Nechť R je těleso a polynom $f \in R[x]$ je normovaný,* $\mathrm{st}(f) \geq 1$. *Zobrazení $\varphi : R \to R[x]/[0]_f$ určené předpisem $\varphi(r) = [r]_f$ je injektivní homomorfismus okruhů.*

Poznámka. Díky předchozí větě můžeme ztotožnit libovolný prvek $r \in R$ s třídou $[r]_f$. Po tomto ztotožnění se R stane podokruhem okruhu $K = R[x]/[0]_f$. Označme $\alpha = [x]_f$. Pro libovolný polynom $g = a_k x^k + a_{k-1} x^{k-1} + \cdots + a_1 x + a_0 \in R[x]$ pak můžeme (v okruhu K) spočítat hodnotu polynomu g v prvku α.

Vnoření tělesa R do okruhu $R[x]/[0]_f$

Věta. *Nechť R je těleso a polynom $f \in R[x]$ je normovaný,* $\mathrm{st}(f) \geq 1$. *Zobrazení $\varphi : R \to R[x]/[0]_f$ určené předpisem $\varphi(r) = [r]_f$ je injektivní homomorfismus okruhů.*

Poznámka. Díky předchozí větě můžeme ztotožnit libovolný prvek $r \in R$ s třídou $[r]_f$. Po tomto ztotožnění se R stane podokruhem okruhu $K = R[x]/[0]_f$. Označme $\alpha = [x]_f$. Pro libovolný polynom $g = a_k x^k + a_{k-1} x^{k-1} + \cdots + a_1 x + a_0 \in R[x]$ pak můžeme (v okruhu K) spočítat hodnotu polynomu g v prvku α. Platí

$$\begin{aligned} g(\alpha) &= a_k \alpha^k + a_{k-1} \alpha^{k-1} + \cdots + a_1 \alpha + a_0 = \\ &= a_k [x]_f^k + a_{k-1} [x]_f^{k-1} + \cdots + a_1 [x]_f + a_0 = \\ &= [a_k x^k]_f + [a_{k-1} x^{k-1}]_f + \cdots + [a_1 x]_f + [a_0]_f = \\ &= [a_k x^k + a_{k-1} x^{k-1} + \cdots + a_1 x + a_0]_f = [g]_f. \end{aligned}$$

Vnoření tělesa R do okruhu $R[x]/[0]_f$

Věta. *Nechť R je těleso a polynom $f \in R[x]$ je normovaný,* $\mathrm{st}(f) \geq 1$. *Zobrazení $\varphi : R \to R[x]/[0]_f$ určené předpisem $\varphi(r) = [r]_f$ je injektivní homomorfismus okruhů.*

Poznámka. Díky předchozí větě můžeme ztotožnit libovolný prvek $r \in R$ s třídou $[r]_f$. Po tomto ztotožnění se R stane podokruhem okruhu $K = R[x]/[0]_f$. Označme $\alpha = [x]_f$. Pro libovolný polynom $g = a_k x^k + a_{k-1} x^{k-1} + \cdots + a_1 x + a_0 \in R[x]$ pak můžeme (v okruhu K) spočítat hodnotu polynomu g v prvku α. Platí

$$\begin{aligned} g(\alpha) &= a_k \alpha^k + a_{k-1} \alpha^{k-1} + \cdots + a_1 \alpha + a_0 = \\ &= a_k [x]_f^k + a_{k-1} [x]_f^{k-1} + \cdots + a_1 [x]_f + a_0 = \\ &= [a_k x^k]_f + [a_{k-1} x^{k-1}]_f + \cdots + [a_1 x]_f + [a_0]_f = \\ &= [a_k x^k + a_{k-1} x^{k-1} + \cdots + a_1 x + a_0]_f = [g]_f. \end{aligned}$$

Speciálně $f(\alpha) = [f]_f = [0]_f$, tedy α je kořen polynomu f.

Vnoření tělesa R do okruhu $R[x]/[0]_f$

Věta. *Nechť R je těleso a polynom $f \in R[x]$ je normovaný,* $\mathrm{st}(f) \geq 1$. *Zobrazení $\varphi : R \to R[x]/[0]_f$ určené předpisem $\varphi(r) = [r]_f$ je injektivní homomorfismus okruhů.*

Poznámka. Díky předchozí větě můžeme ztotožnit libovolný prvek $r \in R$ s třídou $[r]_f$. Po tomto ztotožnění se R stane podokruhem okruhu $K = R[x]/[0]_f$. Označme $\alpha = [x]_f$. Pro libovolný polynom $g = a_k x^k + a_{k-1}x^{k-1} + \cdots + a_1 x + a_0 \in R[x]$ pak můžeme (v okruhu K) spočítat hodnotu polynomu g v prvku α. Platí

$$\begin{aligned} g(\alpha) &= a_k\alpha^k + a_{k-1}\alpha^{k-1} + \cdots + a_1\alpha + a_0 = \\ &= a_k[x]_f^k + a_{k-1}[x]_f^{k-1} + \cdots + a_1[x]_f + a_0 = \\ &= [a_k x^k]_f + [a_{k-1}x^{k-1}]_f + \cdots + [a_1 x]_f + [a_0]_f = \\ &= [a_k x^k + a_{k-1}x^{k-1} + \cdots + a_1 x + a_0]_f = [g]_f. \end{aligned}$$

Speciálně $f(\alpha) = [f]_f = [0]_f$, tedy α je kořen polynomu f. Podle definice je $R[\alpha]$ podokruh okruhu K generovaný množinou $R \cup \{\alpha\}$. Z předchozího výpočtu plyne $R[\alpha] = K$.

Aplikace algebry: samoopravné kódy

Cílem kódování je přenášet informace tak, abychom postřehli, pokud by došlo k jejich zkreslení náhodnou chybou, v ideálním případě dokonce takto vzniklou chybu nejen odhalit, ale i opravit.

Aplikace algebry: samoopravné kódy

Cílem kódování je přenášet informace tak, abychom postřehli, pokud by došlo k jejich zkreslení náhodnou chybou, v ideálním případě dokonce takto vzniklou chybu nejen odhalit, ale i opravit.

Použití: ukládání dat (paměť počítače, CD, DVD, Blue-ray, čárové kódy, QR-kódy), komunikace (digitální TV, vesmírné sondy), atd.

Aplikace algebry: samoopravné kódy

Cílem kódování je přenášet informace tak, abychom postřehli, pokud by došlo k jejich zkreslení náhodnou chybou, v ideálním případě dokonce takto vzniklou chybu nejen odhalit, ale i opravit.

Použití: ukládání dat (paměť počítače, CD, DVD, Blue-ray, čárové kódy, QR-kódy), komunikace (digitální TV, vesmírné sondy), atd.

Přenášená informace bude zapsána pomocí abecedy, která má p písmen (tj. jakýchsi symbolů), kde p je pevně zvolené prvočíslo.

Aplikace algebry: samoopravné kódy

Cílem kódování je přenášet informace tak, abychom postřehli, pokud by došlo k jejich zkreslení náhodnou chybou, v ideálním případě dokonce takto vzniklou chybu nejen odhalit, ale i opravit.

Použití: ukládání dat (paměť počítače, CD, DVD, Blue-ray, čárové kódy, QR-kódy), komunikace (digitální TV, vesmírné sondy), atd.

Přenášená informace bude zapsána pomocí abecedy, která má p písmen (tj. jakýchsi symbolů), kde p je pevně zvolené prvočíslo. Tuto abecedu tedy můžeme ztotožnit s množinou $\mathbb{Z}_p$ všech zbytkových tříd modulo p.

Aplikace algebry: samoopravné kódy

Cílem kódování je přenášet informace tak, abychom postřehli, pokud by došlo k jejich zkreslení náhodnou chybou, v ideálním případě dokonce takto vzniklou chybu nejen odhalit, ale i opravit.

Použití: ukládání dat (paměť počítače, CD, DVD, Blue-ray, čárové kódy, QR-kódy), komunikace (digitální TV, vesmírné sondy), atd.

Přenášená informace bude zapsána pomocí abecedy, která má p písmen (tj. jakýchsi symbolů), kde p je pevně zvolené prvočíslo. Tuto abecedu tedy můžeme ztotožnit s množinou $\mathbb{Z}_p$ všech zbytkových tříd modulo p. Přenášet budeme slova délky n, každé takové kódové slovo $a_1 a_2 a_3 \dots a_{n-1} a_n$ lze tedy chápat jako polynom

$$a = a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_{n-1} x + a_n \in \mathbb{Z}_p[x]$$

stupně $\mathrm{st}(a) < n$.

Aplikace algebry: samoopravné kódy

Cílem kódování je přenášet informace tak, abychom postřehli, pokud by došlo k jejich zkreslení náhodnou chybou, v ideálním případě dokonce takto vzniklou chybu nejen odhalit, ale i opravit.

Použití: ukládání dat (paměť počítače, CD, DVD, Blue-ray, čárové kódy, QR-kódy), komunikace (digitální TV, vesmírné sondy), atd.

Přenášená informace bude zapsána pomocí abecedy, která má p písmen (tj. jakýchsi symbolů), kde p je pevně zvolené prvočíslo. Tuto abecedu tedy můžeme ztotožnit s množinou $\mathbb{Z}_p$ všech zbytkových tříd modulo p. Přenášet budeme slova délky n, každé takové kódové slovo $a_1 a_2 a_3 \dots a_{n-1} a_n$ lze tedy chápat jako polynom

$$a = a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_{n-1} x + a_n \in \mathbb{Z}_p[x]$$

stupně $\mathrm{st}(a) < n$. Číslo n nazýváme délka kódu.

Aplikace algebry: samoopravné kódy

Cílem kódování je přenášet informace tak, abychom postřehli, pokud by došlo k jejich zkreslení náhodnou chybou, v ideálním případě dokonce takto vzniklou chybu nejen odhalit, ale i opravit.

Použití: ukládání dat (paměť počítače, CD, DVD, Blue-ray, čárové kódy, QR-kódy), komunikace (digitální TV, vesmírné sondy), atd.

Přenášená informace bude zapsána pomocí abecedy, která má p písmen (tj. jakýchsi symbolů), kde p je pevně zvolené prvočíslo. Tuto abecedu tedy můžeme ztotožnit s množinou $\mathbb{Z}_p$ všech zbytkových tříd modulo p. Přenášet budeme slova délky n, každé takové kódové slovo $a_1 a_2 a_3 \dots a_{n-1} a_n$ lze tedy chápat jako polynom

$$a = a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_{n-1} x + a_n \in \mathbb{Z}_p[x]$$

stupně $\mathrm{st}(a) < n$. Číslo n nazýváme délka kódu.

Kdyby každý polynom stupně menšího než n bylo některé z kódových slov, tak bychom nemohli postřehnout, že při přenosu došlo k nějaké náhodné chybě.

Polynomiální kód délky n daný polynomem $g \in \mathbb{Z}_p[x]$

Máme tedy pevně zvolené prvočíslo p a přirozené číslo n.

Polynomiální kód délky n daný polynomem $g \in \mathbb{Z}_p[x]$

Máme tedy pevně zvolené prvočíslo p a přirozené číslo n.

Zafixujme také polynom $g \in \mathbb{Z}_p[x]$ stupně $\mathrm{st}(g) = k < n$.

Polynomiální kód délky n daný polynomem $g \in \mathbb{Z}_p[x]$

Máme tedy pevně zvolené prvočíslo p a přirozené číslo n.

Zafixujme také polynom $g \in \mathbb{Z}_p[x]$ stupně $\mathrm{st}(g) = k < n$.

Kódová slova budou ty polynomy $a \in \mathbb{Z}_p[x]$ stupně $\mathrm{st}(a) < n$, které jsou dělitelné polynomem g v okruhu $\mathbb{Z}_p[x]$, jsou to tedy polynomy $a = g \cdot h$, kde $h \in \mathbb{Z}_p[x]$ je libovolný polynom stupně $\mathrm{st}(h) < n - k$.

Polynomiální kód délky n daný polynomem $g \in \mathbb{Z}_p[x]$

Máme tedy pevně zvolené prvočíslo p a přirozené číslo n.

Zafixujme také polynom $g \in \mathbb{Z}_p[x]$ stupně $\mathrm{st}(g) = k < n$.

Kódová slova budou ty polynomy $a \in \mathbb{Z}_p[x]$ stupně $\mathrm{st}(a) < n$, které jsou dělitelné polynomem g v okruhu $\mathbb{Z}_p[x]$, jsou to tedy polynomy $a = g \cdot h$, kde $h \in \mathbb{Z}_p[x]$ je libovolný polynom stupně $\mathrm{st}(h) < n - k$.

Pokud chceme odeslat zprávu zapsanou pomocí $n - k$ písmen, tj. polynom $b = b_1 x^{n-k-1} + \cdots + b_{n-k-1} x + b_{n-k} \in \mathbb{Z}_p[x]$ stupně $\mathrm{st}(b) < n - k$,

Polynomiální kód délky n daný polynomem $g \in \mathbb{Z}_p[x]$

Máme tedy pevně zvolené prvočíslo p a přirozené číslo n.

Zafixujme také polynom $g \in \mathbb{Z}_p[x]$ stupně $\mathrm{st}(g) = k < n$.

Kódová slova budou ty polynomy $a \in \mathbb{Z}_p[x]$ stupně $\mathrm{st}(a) < n$, které jsou dělitelné polynomem g v okruhu $\mathbb{Z}_p[x]$, jsou to tedy polynomy $a = g \cdot h$, kde $h \in \mathbb{Z}_p[x]$ je libovolný polynom stupně $\mathrm{st}(h) < n - k$.

Pokud chceme odeslat zprávu zapsanou pomocí $n - k$ písmen, tj. polynom $b = b_1 x^{n-k-1} + \cdots + b_{n-k-1} x + b_{n-k} \in \mathbb{Z}_p[x]$ stupně $\mathrm{st}(b) < n - k$, vydělíme polynom $x^k \cdot b$ polynomem g se zbytkem a dostaneme polynomy q, $r \in \mathbb{Z}_p[x]$ tak, že $x^k \cdot b = g \cdot q + r$, kde $\mathrm{st}(r) < k$.

Polynomiální kód délky n daný polynomem $g \in \mathbb{Z}_p[x]$

Máme tedy pevně zvolené prvočíslo p a přirozené číslo n.

Zafixujme také polynom $g \in \mathbb{Z}_p[x]$ stupně $\mathrm{st}(g) = k < n$.

Kódová slova budou ty polynomy $a \in \mathbb{Z}_p[x]$ stupně $\mathrm{st}(a) < n$, které jsou dělitelné polynomem g v okruhu $\mathbb{Z}_p[x]$, jsou to tedy polynomy $a = g \cdot h$, kde $h \in \mathbb{Z}_p[x]$ je libovolný polynom stupně $\mathrm{st}(h) < n - k$.

Pokud chceme odeslat zprávu zapsanou pomocí $n - k$ písmen, tj. polynom $b = b_1 x^{n-k-1} + \cdots + b_{n-k-1} x + b_{n-k} \in \mathbb{Z}_p[x]$ stupně $\mathrm{st}(b) < n - k$, vydělíme polynom $x^k \cdot b$ polynomem g se zbytkem a dostaneme polynomy q, $r \in \mathbb{Z}_p[x]$ tak, že $x^k \cdot b = g \cdot q + r$, kde $\mathrm{st}(r) < k$.

Odešleme pak polynom $g \cdot q = x^k \cdot b - r$.

Polynomiální kód délky n daný polynomem $g \in \mathbb{Z}_p[x]$

Máme tedy pevně zvolené prvočíslo p a přirozené číslo n.

Zafixujme také polynom $g \in \mathbb{Z}_p[x]$ stupně $\mathrm{st}(g) = k < n$.

Kódová slova budou ty polynomy $a \in \mathbb{Z}_p[x]$ stupně $\mathrm{st}(a) < n$, které jsou dělitelné polynomem g v okruhu $\mathbb{Z}_p[x]$, jsou to tedy polynomy $a = g \cdot h$, kde $h \in \mathbb{Z}_p[x]$ je libovolný polynom stupně $\mathrm{st}(h) < n - k$.

Pokud chceme odeslat zprávu zapsanou pomocí $n - k$ písmen, tj. polynom $b = b_1 x^{n-k-1} + \cdots + b_{n-k-1} x + b_{n-k} \in \mathbb{Z}_p[x]$ stupně $\mathrm{st}(b) < n - k$, vydělíme polynom $x^k \cdot b$ polynomem g se zbytkem a dostaneme polynomy q, $r \in \mathbb{Z}_p[x]$ tak, že $x^k \cdot b = g \cdot q + r$, kde $\mathrm{st}(r) < k$.

Odešleme pak polynom $g \cdot q = x^k \cdot b - r$.

Každé kódové slovo se tedy skládá z $n - k$ významových písmen (daných polynomem b) následovaných k kontrolními písmeny (daných polynomem $-r$).

Polynomiální kód délky n daný polynomem $g \in \mathbb{Z}_p[x]$

Máme tedy pevně zvolené prvočíslo p a přirozené číslo n.

Zafixujme také polynom $g \in \mathbb{Z}_p[x]$ stupně $\mathrm{st}(g) = k < n$.

Kódová slova budou ty polynomy $a \in \mathbb{Z}_p[x]$ stupně $\mathrm{st}(a) < n$, které jsou dělitelné polynomem g v okruhu $\mathbb{Z}_p[x]$, jsou to tedy polynomy $a = g \cdot h$, kde $h \in \mathbb{Z}_p[x]$ je libovolný polynom stupně $\mathrm{st}(h) < n - k$.

Pokud chceme odeslat zprávu zapsanou pomocí $n - k$ písmen, tj. polynom $b = b_1 x^{n-k-1} + \cdots + b_{n-k-1} x + b_{n-k} \in \mathbb{Z}_p[x]$ stupně $\mathrm{st}(b) < n - k$, vydělíme polynom $x^k \cdot b$ polynomem g se zbytkem a dostaneme polynomy q, $r \in \mathbb{Z}_p[x]$ tak, že $x^k \cdot b = g \cdot q + r$, kde $\mathrm{st}(r) < k$.

Odešleme pak polynom $g \cdot q = x^k \cdot b - r$.

Každé kódové slovo se tedy skládá z $n - k$ významových písmen (daných polynomem b) následovaných k kontrolními písmeny (daných polynomem $-r$). Je však nutné vhodně zvolit polynom g.

Polynomiální kód délky n daný polynomem $g \in \mathbb{Z}_p[x]$

Máme tedy pevně zvolené prvočíslo p a přirozené číslo n.

Zafixujme také polynom $g \in \mathbb{Z}_p[x]$ stupně $\mathrm{st}(g) = k < n$.

Kódová slova budou ty polynomy $a \in \mathbb{Z}_p[x]$ stupně $\mathrm{st}(a) < n$, které jsou dělitelné polynomem g v okruhu $\mathbb{Z}_p[x]$, jsou to tedy polynomy $a = g \cdot h$, kde $h \in \mathbb{Z}_p[x]$ je libovolný polynom stupně $\mathrm{st}(h) < n - k$.

Pokud chceme odeslat zprávu zapsanou pomocí $n - k$ písmen, tj. polynom $b = b_1 x^{n-k-1} + \cdots + b_{n-k-1} x + b_{n-k} \in \mathbb{Z}_p[x]$ stupně $\mathrm{st}(b) < n - k$, vydělíme polynom $x^k \cdot b$ polynomem g se zbytkem a dostaneme polynomy q, $r \in \mathbb{Z}_p[x]$ tak, že $x^k \cdot b = g \cdot q + r$, kde $\mathrm{st}(r) < k$.

Odešleme pak polynom $g \cdot q = x^k \cdot b - r$.

Každé kódové slovo se tedy skládá z $n - k$ významových písmen (daných polynomem b) následovaných k kontrolními písmeny (daných polynomem $-r$). Je však nutné vhodně zvolit polynom g. Určitě by nebyla vhodná volba $g = x^k$, protože pak bychom každou zprávu b doplnili nulovým polynomem.

Příklad pro prvočíslo $p = 2$, tedy $\mathbb{Z}_2 = \{0, 1\}$

Zvolme polynom $g = x + 1 \in \mathbb{Z}_2[x]$, tedy $k = \mathrm{st}(g) = 1$.

Příklad pro prvočíslo $p = 2$, tedy $\mathbb{Z}_2 = \{0, 1\}$

Zvolme polynom $g = x + 1 \in \mathbb{Z}_2[x]$, tedy $k = \mathrm{st}(g) = 1$.

Zvolme libovolnou délku kódu $n > 1$.

Příklad pro prvočíslo $p = 2$, tedy $\mathbb{Z}_2 = \{0, 1\}$

Zvolme polynom $g = x + 1 \in \mathbb{Z}_2[x]$, tedy $k = \mathrm{st}(g) = 1$.

Zvolme libovolnou délku kódu $n > 1$.

Odesílanou zprávou je nějaký polynom $b \in \mathbb{Z}_2[x]$ stupně $\mathrm{st}(b) < n - 1$.

Příklad pro prvočíslo $p = 2$, tedy $\mathbb{Z}_2 = \{0, 1\}$

Zvolme polynom $g = x + 1 \in \mathbb{Z}_2[x]$, tedy $k = \mathrm{st}(g) = 1$.

Zvolme libovolnou délku kódu $n > 1$.

Odesílanou zprávou je nějaký polynom $b \in \mathbb{Z}_2[x]$ stupně $\mathrm{st}(b) < n - 1$.

Naše kódová slova se tedy budou skládat z $n - 1$ významových písmen (to jsou koeficienty polynomu b) následovaných jedním kontrolním písmenem.

Příklad pro prvočíslo $p = 2$, tedy $\mathbb{Z}_2 = \{0, 1\}$

Zvolme polynom $g = x + 1 \in \mathbb{Z}_2[x]$, tedy $k = \mathrm{st}(g) = 1$.
Zvolme libovolnou délku kódu $n > 1$.
Odesílanou zprávou je nějaký polynom $b \in \mathbb{Z}_2[x]$ stupně $\mathrm{st}(b) < n - 1$.
Naše kódová slova se tedy budou skládat z $n - 1$ významových písmen (to jsou koeficienty polynomu b) následovaných jedním kontrolním písmenem. Kontrolní písmeno určujeme takto: polynom $x \cdot b$ vydělíme polynomem $g = x + 1$ se zbytkem a dostaneme polynomy q, $r \in \mathbb{Z}_2[x]$ tak, že

$$x^k \cdot b = g \cdot q + r = (x + 1) \cdot q + r,$$

kde $\mathrm{st}(r) < k = 1$.

Příklad pro prvočíslo $p = 2$, tedy $\mathbb{Z}_2 = \{0, 1\}$

Zvolme polynom $g = x + 1 \in \mathbb{Z}_2[x]$, tedy $k = \mathrm{st}(g) = 1$.
Zvolme libovolnou délku kódu $n > 1$.
Odesílanou zprávou je nějaký polynom $b \in \mathbb{Z}_2[x]$ stupně $\mathrm{st}(b) < n - 1$.
Naše kódová slova se tedy budou skládat z $n - 1$ významových písmen (to jsou koeficienty polynomu b) následovaných jedním kontrolním písmenem. Kontrolní písmeno určujeme takto: polynom $x \cdot b$ vydělíme polynomem $g = x + 1$ se zbytkem a dostaneme polynomy q, $r \in \mathbb{Z}_2[x]$ tak, že

$$x^k \cdot b = g \cdot q + r = (x + 1) \cdot q + r,$$

kde $\mathrm{st}(r) < k = 1$.
Tedy polynom $r \in \mathbb{Z}_2[x]$ je konstantní, tj. $r \in \{0, 1\}$.

Příklad pro prvočíslo $p = 2$, tedy $\mathbb{Z}_2 = \{0, 1\}$

Zvolme polynom $g = x + 1 \in \mathbb{Z}_2[x]$, tedy $k = \mathrm{st}(g) = 1$.
Zvolme libovolnou délku kódu $n > 1$.
Odesílanou zprávou je nějaký polynom $b \in \mathbb{Z}_2[x]$ stupně $\mathrm{st}(b) < n - 1$.
Naše kódová slova se tedy budou skládat z $n - 1$ významových písmen (to jsou koeficienty polynomu b) následovaných jedním kontrolním písmenem. Kontrolní písmeno určujeme takto: polynom $x \cdot b$ vydělíme polynomem $g = x + 1$ se zbytkem a dostaneme polynomy q, $r \in \mathbb{Z}_2[x]$ tak, že

$$x^k \cdot b = g \cdot q + r = (x + 1) \cdot q + r,$$

kde $\mathrm{st}(r) < k = 1$.
Tedy polynom $r \in \mathbb{Z}_2[x]$ je konstantní, tj. $r \in \{0, 1\}$. Dosazením $x = 1$ dostaneme $r(1) = b(1)$, a proto $r = b(1)$.

Příklad pro prvočíslo $p = 2$, tedy $\mathbb{Z}_2 = \{0, 1\}$

Zvolme polynom $g = x + 1 \in \mathbb{Z}_2[x]$, tedy $k = \mathrm{st}(g) = 1$.
Zvolme libovolnou délku kódu $n > 1$.
Odesílanou zprávou je nějaký polynom $b \in \mathbb{Z}_2[x]$ stupně $\mathrm{st}(b) < n - 1$.
Naše kódová slova se tedy budou skládat z $n - 1$ významových písmen (to jsou koeficienty polynomu b) následovaných jedním kontrolním písmenem. Kontrolní písmeno určujeme takto: polynom $x \cdot b$ vydělíme polynomem $g = x + 1$ se zbytkem a dostaneme polynomy q, $r \in \mathbb{Z}_2[x]$ tak, že

$$x^k \cdot b = g \cdot q + r = (x + 1) \cdot q + r,$$

kde $\mathrm{st}(r) < k = 1$.
Tedy polynom $r \in \mathbb{Z}_2[x]$ je konstantní, tj. $r \in \{0, 1\}$. Dosazením $x = 1$ dostaneme $r(1) = b(1)$, a proto $r = b(1)$.
Protože $b(1) = 0$, má-li odesílaná zpráva sudý počet jedniček, a $b(1) = 1$, má-li odesílaná zpráva lichý počet jedniček, doplňujeme zprávu jedním písmenem tak, aby celkový počet jedniček byl sudý.

Příklad pro prvočíslo $p = 2$, tedy $\mathbb{Z}_2 = \{0, 1\}$

Zvolme polynom $g = x + 1 \in \mathbb{Z}_2[x]$, tedy $k = \mathrm{st}(g) = 1$.
Zvolme libovolnou délku kódu $n > 1$.
Odesílanou zprávou je nějaký polynom $b \in \mathbb{Z}_2[x]$ stupně $\mathrm{st}(b) < n - 1$.
Naše kódová slova se tedy budou skládat z $n - 1$ významových písmen (to jsou koeficienty polynomu b) následovaných jedním kontrolním písmenem. Kontrolní písmeno určujeme takto: polynom $x \cdot b$ vydělíme polynomem $g = x + 1$ se zbytkem a dostaneme polynomy q, $r \in \mathbb{Z}_2[x]$ tak, že

$$x^k \cdot b = g \cdot q + r = (x + 1) \cdot q + r,$$

kde $\mathrm{st}(r) < k = 1$.
Tedy polynom $r \in \mathbb{Z}_2[x]$ je konstantní, tj. $r \in \{0, 1\}$. Dosazením $x = 1$ dostaneme $r(1) = b(1)$, a proto $r = b(1)$.
Protože $b(1) = 0$, má-li odesílaná zpráva sudý počet jedniček, a $b(1) = 1$, má-li odesílaná zpráva lichý počet jedniček, doplňujeme zprávu jedním písmenem tak, aby celkový počet jedniček byl sudý.
Kód tedy pozná, že došlo k jedné chybě, opravit ji neumí.

Příklad pro prvočíslo $p = 2$, tedy $\mathbb{Z}_2 = \{0, 1\}$

Zvolme polynom $g = x + 1 \in \mathbb{Z}_2[x]$, tedy $k = \mathrm{st}(g) = 1$.
Zvolme libovolnou délku kódu $n > 1$.
Odesílanou zprávou je nějaký polynom $b \in \mathbb{Z}_2[x]$ stupně $\mathrm{st}(b) < n - 1$.
Naše kódová slova se tedy budou skládat z $n - 1$ významových písmen (to jsou koeficienty polynomu b) následovaných jedním kontrolním písmenem. Kontrolní písmeno určujeme takto: polynom $x \cdot b$ vydělíme polynomem $g = x + 1$ se zbytkem a dostaneme polynomy q, $r \in \mathbb{Z}_2[x]$ tak, že

$$x^k \cdot b = g \cdot q + r = (x + 1) \cdot q + r,$$

kde $\mathrm{st}(r) < k = 1$.
Tedy polynom $r \in \mathbb{Z}_2[x]$ je konstantní, tj. $r \in \{0, 1\}$. Dosazením $x = 1$ dostaneme $r(1) = b(1)$, a proto $r = b(1)$.
Protože $b(1) = 0$, má-li odesílaná zpráva sudý počet jedniček, a $b(1) = 1$, má-li odesílaná zpráva lichý počet jedniček, doplňujeme zprávu jedním písmenem tak, aby celkový počet jedniček byl sudý. Kód tedy pozná, že došlo k jedné chybě, opravit ji neumí. Pokud došlo ke dvěma chybám, nic nepozná.

Metrický prostor, Hammingova vzdálenost kódových slov

Metrickým prostorem rozumíme nějakou neprázdnou množinu M (jejím prvkům říkáme body) spolu s metrikou na množině M, což je zobrazení $\rho : M \times M \to \mathbb{R}_0^+$, kde $\mathbb{R}_0^+$ značí množinu nezáporných reálných čísel, splňující pro každé $x, y, z \in M$

- $\rho(x, y) = 0 \iff x = y$,
- $\rho(x, y) = \rho(y, x)$,
- $\rho(x, y) + \rho(y, z) \geq \rho(x, z)$.

Metrický prostor, Hammingova vzdálenost kódových slov

Metrickým prostorem rozumíme nějakou neprázdnou množinu M (jejím prvkům říkáme body) spolu s metrikou na množině M, což je zobrazení $\rho : M \times M \to \mathbb{R}_0^+$, kde $\mathbb{R}_0^+$ značí množinu nezáporných reálných čísel, splňující pro každé $x, y, z \in M$

- $\rho(x, y) = 0 \iff x = y$,
- $\rho(x, y) = \rho(y, x)$,
- $\rho(x, y) + \rho(y, z) \geq \rho(x, z)$.

Při práci v metrickém prostoru můžeme používat svou geometrickou intuici, například mluvit o koulích s daným středem a daným poloměrem (jde o množinu bodů, jejichž vzdálenost od daného středu není větší než daný poloměr).

Metrický prostor, Hammingova vzdálenost kódových slov

Metrickým prostorem rozumíme nějakou neprázdnou množinu M (jejím prvkům říkáme body) spolu s metrikou na množině M, což je zobrazení $\rho : M \times M \to \mathbb{R}_0^+$, kde $\mathbb{R}_0^+$ značí množinu nezáporných reálných čísel, splňující pro každé $x, y, z \in M$

- $\rho(x, y) = 0 \iff x = y$,
- $\rho(x, y) = \rho(y, x)$,
- $\rho(x, y) + \rho(y, z) \geq \rho(x, z)$.

Při práci v metrickém prostoru můžeme používat svou geometrickou intuici, například mluvit o koulích s daným středem a daným poloměrem (jde o množinu bodů, jejichž vzdálenost od daného středu není větší než daný poloměr).

Pro každé dva polynomy a, $b \in \mathbb{Z}_p[x]$ stupnů $\mathrm{st}(a) < n$, $\mathrm{st}(b) < n$, definujeme jejich Hammingovu vzdálenost jako počet nenulových koeficientů rozdílu $a - b$, tj. počet koeficientů, v nichž se oba polynomy liší.

Metrický prostor, Hammingova vzdálenost kódových slov

Metrickým prostorem rozumíme nějakou neprázdnou množinu M (jejím prvkům říkáme body) spolu s metrikou na množině M, což je zobrazení $\rho : M \times M \to \mathbb{R}_0^+$, kde $\mathbb{R}_0^+$ značí množinu nezáporných reálných čísel, splňující pro každé $x, y, z \in M$

- $\rho(x, y) = 0 \iff x = y$,
- $\rho(x, y) = \rho(y, x)$,
- $\rho(x, y) + \rho(y, z) \geq \rho(x, z)$.

Při práci v metrickém prostoru můžeme používat svou geometrickou intuici, například mluvit o koulích s daným středem a daným poloměrem (jde o množinu bodů, jejichž vzdálenost od daného středu není větší než daný poloměr).

Pro každé dva polynomy a, $b \in \mathbb{Z}_p[x]$ stupnů $\mathrm{st}(a) < n$, $\mathrm{st}(b) < n$, definujeme jejich Hammingovu vzdálenost jako počet nenulových koeficientů rozdílu $a - b$, tj. počet koeficientů, v nichž se oba polynomy liší. Uvědomte si, že jde o metrický prostor.

Užití Hammingovy vzdálenosti kódových slov

Máme-li být schopni postřehnout, že došlo k chybě, pokud při přenosu bylo právě na jedné pozici přenášené písmeno náhodné změněno, je třeba, aby vzdálenost libovolných dvou různých kódových slov byla alespoň 2.

Užití Hammingovy vzdálenosti kódových slov

Máme-li být schopni postřehnout, že došlo k chybě, pokud při přenosu bylo právě na jedné pozici přenášené písmeno náhodné změněno, je třeba, aby vzdálenost libovolných dvou různých kódových slov byla alespoň 2.

Pokud tato vzdálenost libovolných dvou různých kódových slov bude alespoň 3, budeme dokonce schopni takovou chybu i opravit.

Užití Hammingovy vzdálenosti kódových slov

Máme-li být schopni postřehnout, že došlo k chybě, pokud při přenosu bylo právě na jedné pozici přenášené písmeno náhodné změněno, je třeba, aby vzdálenost libovolných dvou různých kódových slov byla alespoň 2.

Pokud tato vzdálenost libovolných dvou různých kódových slov bude alespoň 3, budeme dokonce schopni takovou chybu i opravit.

Obecněji, je-li pro nějaké $t \in \mathbb{N}$ vzdálenost libovolných dvou různých kódových slov alespoň $t + 1$, pak lze chybu detekovat, když došlo při přenosu ke změně na nejvýše t pozicích.

Užití Hammingovy vzdálenosti kódových slov

Máme-li být schopni postřehnout, že došlo k chybě, pokud při přenosu bylo právě na jedné pozici přenášené písmeno náhodné změněno, je třeba, aby vzdálenost libovolných dvou různých kódových slov byla alespoň 2.

Pokud tato vzdálenost libovolných dvou různých kódových slov bude alespoň 3, budeme dokonce schopni takovou chybu i opravit.

Obecněji, je-li pro nějaké $t \in \mathbb{N}$ vzdálenost libovolných dvou různých kódových slov alespoň $t + 1$, pak lze chybu detekovat, když došlo při přenosu ke změně na nejvýše t pozicích. Je-li tato vzdálenost alespoň $2t + 1$, pak takovou chybu lze dokonce i správně opravit.

Užití Hammingovy vzdálenosti kódových slov

Máme-li být schopni postřehnout, že došlo k chybě, pokud při přenosu bylo právě na jedné pozici přenášené písmeno náhodné změněno, je třeba, aby vzdálenost libovolných dvou různých kódových slov byla alespoň 2.

Pokud tato vzdálenost libovolných dvou různých kódových slov bude alespoň 3, budeme dokonce schopni takovou chybu i opravit.

Obecněji, je-li pro nějaké $t \in \mathbb{N}$ vzdálenost libovolných dvou různých kódových slov alespoň $t + 1$, pak lze chybu detekovat, když došlo při přenosu ke změně na nejvýše t pozicích. Je-li tato vzdálenost alespoň $2t + 1$, pak takovou chybu lze dokonce i správně opravit.

Protože u polynomiálního kódu je rozdíl libovolných dvou kódových slov opět kódové slovo, lze místo o nejmenší vzdálenosti dvou různých kódových slov hovořit o nejmenší vzdálenosti nenulového kódového slova od nuly.

Příklad

Zvolme $p = 2$, tedy písmena jsou 0 a 1.

Příklad

Zvolme $p = 2$, tedy písmena jsou 0 a 1. Dále položme $n = 5$, $g = x^2 + x + 1$.

Příklad

Zvolme $p = 2$, tedy písmena jsou 0 a 1. Dále položme $n = 5$, $g = x^2 + x + 1$. Pak kódová slova jsou polynomy

$$0, \quad x^2 + x + 1, \quad x^3 + x^2 + x, \quad x^3 + 1,$$
$$x^4 + x^3 + x^2, \quad x^4 + x^3 + x + 1, \quad x^4 + x, \quad x^4 + x^2 + 1.$$

Příklad

Zvolme $p = 2$, tedy písmena jsou 0 a 1. Dále položme $n = 5$, $g = x^2 + x + 1$. Pak kódová slova jsou polynomy

$$0, \quad x^2 + x + 1, \quad x^3 + x^2 + x, \quad x^3 + 1,$$
$$x^4 + x^3 + x^2, \quad x^4 + x^3 + x + 1, \quad x^4 + x, \quad x^4 + x^2 + 1.$$

Budeme-li polynomy psát jako posloupnosti koeficientů, budeme kódovat takto:

$$\begin{aligned} 000 &\mapsto 00000, & 100 &\mapsto 10010, \\ 001 &\mapsto 00111, & 101 &\mapsto 10101, \\ 010 &\mapsto 01001, & 110 &\mapsto 11011, \\ 011 &\mapsto 01110, & 111 &\mapsto 11100. \end{aligned}$$

Příklad

Zvolme $p = 2$, tedy písmena jsou 0 a 1. Dále položme $n = 5$, $g = x^2 + x + 1$. Pak kódová slova jsou polynomy

$$0, \quad x^2 + x + 1, \quad x^3 + x^2 + x, \quad x^3 + 1,$$
$$x^4 + x^3 + x^2, \quad x^4 + x^3 + x + 1, \quad x^4 + x, \quad x^4 + x^2 + 1.$$

Budeme-li polynomy psát jako posloupnosti koeficientů, budeme kódovat takto:

$$\begin{aligned} 000 &\mapsto 00000, & 100 &\mapsto 10010, \\ 001 &\mapsto 00111, & 101 &\mapsto 10101, \\ 010 &\mapsto 01001, & 110 &\mapsto 11011, \\ 011 &\mapsto 01110, & 111 &\mapsto 11100. \end{aligned}$$

Je ihned vidět, že nejmenší vzdálenost nenulového kódového slova od nuly je 2, jsme tedy schopni detekovat chybu na jedné pozici.

Příklad

Zvolme $p = 2$, tedy písmena jsou 0 a 1. Dále položme $n = 5$, $g = x^2 + x + 1$. Pak kódová slova jsou polynomy

$$0, \quad x^2 + x + 1, \quad x^3 + x^2 + x, \quad x^3 + 1,$$
$$x^4 + x^3 + x^2, \quad x^4 + x^3 + x + 1, \quad x^4 + x, \quad x^4 + x^2 + 1.$$

Budeme-li polynomy psát jako posloupnosti koeficientů, budeme kódovat takto:

$$\begin{aligned} 000 &\mapsto 00000, & 100 &\mapsto 10010, \\ 001 &\mapsto 00111, & 101 &\mapsto 10101, \\ 010 &\mapsto 01001, & 110 &\mapsto 11011, \\ 011 &\mapsto 01110, & 111 &\mapsto 11100. \end{aligned}$$

Je ihned vidět, že nejmenší vzdálenost nenulového kódového slova od nuly je 2, jsme tedy schopni detekovat chybu na jedné pozici. Opravit tuto chybu nejsme obecně schopni, například posloupnost 01000 by mohla vzniknout jednou chybou na druhé pozici anebo jednou chybou na páté pozici.

Kód opravující chybu na jedné pozici

Věta. *Nechť p je prvočíslo a $f \in \mathbb{Z}_p[x]$ je normovaný ireducibilní polynom, $m = \mathrm{st}(f) > 1$.*

Kód opravující chybu na jedné pozici

Věta. *Nechť p je prvočíslo a $f \in \mathbb{Z}_p[x]$ je normovaný ireducibilní polynom, $m = \mathrm{st}(f) > 1$. Předpokládejme, že polynom f je zvolen tak, že v tělese $K = \mathbb{Z}_p[x]/[0]_f$ je prvek $\alpha = [x]_f \in K$ generátor multiplikativní grupy $(K^\times, \cdot)$ tělesa K.*

Kód opravující chybu na jedné pozici

Věta. *Nechť p je prvočíslo a $f \in \mathbb{Z}_p[x]$ je normovaný ireducibilní polynom, $m = \mathrm{st}(f) > 1$. Předpokládejme, že polynom f je zvolen tak, že v tělese $K = \mathbb{Z}_p[x]/[0]_f$ je prvek $\alpha = [x]_f \in K$ generátor multiplikativní grupy $(K^\times, \cdot)$ tělesa K. Pak polynomiální kód délky $n = \frac{p^m-1}{p-1}$ daný polynomem f je schopen opravit chybu na jedné pozici.*

Kód opravující chybu na jedné pozici

Věta. *Nechť p je prvočíslo a $f \in \mathbb{Z}_p[x]$ je normovaný ireducibilní polynom, $m = \mathrm{st}(f) > 1$. Předpokládejme, že polynom f je zvolen tak, že v tělese $K = \mathbb{Z}_p[x]/[0]_f$ je prvek $\alpha = [x]_f \in K$ generátor multiplikativní grupy $(K^\times, \cdot)$ tělesa K. Pak polynomiální kód délky $n = \frac{p^m-1}{p-1}$ daný polynomem f je schopen opravit chybu na jedné pozici.*

Důkaz. Platí $\mathrm{st}(f) = m < 1 + p + \cdots + p^{m-1} = n$. Stačí ukázat, že žádné kódové slovo nemá vzdálenost 1 nebo 2 od nuly.

Kód opravující chybu na jedné pozici

Věta. *Nechť p je prvočíslo a $f \in \mathbb{Z}_p[x]$ je normovaný ireducibilní polynom, $m = \mathrm{st}(f) > 1$. Předpokládejme, že polynom f je zvolen tak, že v tělese $K = \mathbb{Z}_p[x]/[0]_f$ je prvek $\alpha = [x]_f \in K$ generátor multiplikativní grupy $(K^\times, \cdot)$ tělesa K. Pak polynomiální kód délky $n = \frac{p^m-1}{p-1}$ daný polynomem f je schopen opravit chybu na jedné pozici.*

Důkaz. Platí $\mathrm{st}(f) = m < 1 + p + \cdots + p^{m-1} = n$. Stačí ukázat, že žádné kódové slovo nemá vzdálenost 1 nebo 2 od nuly. Sporem: předpokládejme, že pro nějaká $0 \leq i < j < n$, $a \in \mathbb{Z}_p^\times$, $b \in \mathbb{Z}_p$ je polynom $ax^j + bx^i$ kódové slovo.

Kód opravující chybu na jedné pozici

Věta. *Nechť p je prvočíslo a $f \in \mathbb{Z}_p[x]$ je normovaný ireducibilní polynom, $m = \mathrm{st}(f) > 1$. Předpokládejme, že polynom f je zvolen tak, že v tělese $K = \mathbb{Z}_p[x]/[0]_f$ je prvek $\alpha = [x]_f \in K$ generátor multiplikativní grupy $(K^\times, \cdot)$ tělesa K. Pak polynomiální kód délky $n = \frac{p^m-1}{p-1}$ daný polynomem f je schopen opravit chybu na jedné pozici.*

Důkaz. Platí $\mathrm{st}(f) = m < 1 + p + \cdots + p^{m-1} = n$. Stačí ukázat, že žádné kódové slovo nemá vzdálenost 1 nebo 2 od nuly. Sporem: předpokládejme, že pro nějaká $0 \leq i < j < n$, $a \in \mathbb{Z}_p^\times$, $b \in \mathbb{Z}_p$ je polynom $ax^j + bx^i$ kódové slovo. Pak $f \mid ax^j + bx^i$, tj.
$0 = [ax^j + bx^i]_f = a\alpha^j + b\alpha^i = a\alpha^i(\alpha^{j-i} - b \cdot a^{-1})$.

Kód opravující chybu na jedné pozici

Věta. *Nechť p je prvočíslo a $f \in \mathbb{Z}_p[x]$ je normovaný ireducibilní polynom, $m = \mathrm{st}(f) > 1$. Předpokládejme, že polynom f je zvolen tak, že v tělese $K = \mathbb{Z}_p[x]/[0]_f$ je prvek $\alpha = [x]_f \in K$ generátor multiplikativní grupy $(K^\times, \cdot)$ tělesa K. Pak polynomiální kód délky $n = \frac{p^m-1}{p-1}$ daný polynomem f je schopen opravit chybu na jedné pozici.*

Důkaz. Platí $\mathrm{st}(f) = m < 1 + p + \cdots + p^{m-1} = n$. Stačí ukázat, že žádné kódové slovo nemá vzdálenost 1 nebo 2 od nuly. Sporem: předpokládejme, že pro nějaká $0 \leq i < j < n$, $a \in \mathbb{Z}_p^\times$, $b \in \mathbb{Z}_p$ je polynom $ax^j + bx^i$ kódové slovo. Pak $f \mid ax^j + bx^i$, tj. $0 = [ax^j + bx^i]_f = a\alpha^j + b\alpha^i = a\alpha^i(\alpha^{j-i} - b \cdot a^{-1})$. Protože K je těleso a platí $a\alpha^i \neq 0$, plyne odtud $\alpha^{j-i} = b \cdot a^{-1}$.

Kód opravující chybu na jedné pozici

Věta. *Nechť p je prvočíslo a $f \in \mathbb{Z}_p[x]$ je normovaný ireducibilní polynom, $m = \mathrm{st}(f) > 1$. Předpokládejme, že polynom f je zvolen tak, že v tělese $K = \mathbb{Z}_p[x]/[0]_f$ je prvek $\alpha = [x]_f \in K$ generátor multiplikativní grupy $(K^\times, \cdot)$ tělesa K. Pak polynomiální kód délky $n = \frac{p^m-1}{p-1}$ daný polynomem f je schopen opravit chybu na jedné pozici.*

Důkaz. Platí $\mathrm{st}(f) = m < 1 + p + \cdots + p^{m-1} = n$. Stačí ukázat, že žádné kódové slovo nemá vzdálenost 1 nebo 2 od nuly. Sporem: předpokládejme, že pro nějaká $0 \leq i < j < n$, $a \in \mathbb{Z}_p^\times$, $b \in \mathbb{Z}_p$ je polynom $ax^j + bx^i$ kódové slovo. Pak $f \mid ax^j + bx^i$, tj. $0 = [ax^j + bx^i]_f = a\alpha^j + b\alpha^i = a\alpha^i(\alpha^{j-i} - b \cdot a^{-1})$. Protože K je těleso a platí $a\alpha^i \neq 0$, plyne odtud $\alpha^{j-i} = b \cdot a^{-1}$. Proto $b \neq 0$, a tedy $b \cdot a^{-1} \in \mathbb{Z}_p^\times$.

Kód opravující chybu na jedné pozici

Věta. *Nechť p je prvočíslo a $f \in \mathbb{Z}_p[x]$ je normovaný ireducibilní polynom, $m = \mathrm{st}(f) > 1$. Předpokládejme, že polynom f je zvolen tak, že v tělese $K = \mathbb{Z}_p[x]/[0]_f$ je prvek $\alpha = [x]_f \in K$ generátor multiplikativní grupy $(K^\times, \cdot)$ tělesa K. Pak polynomiální kód délky $n = \frac{p^m-1}{p-1}$ daný polynomem f je schopen opravit chybu na jedné pozici.*

Důkaz. Platí $\mathrm{st}(f) = m < 1 + p + \cdots + p^{m-1} = n$. Stačí ukázat, že žádné kódové slovo nemá vzdálenost 1 nebo 2 od nuly. Sporem: předpokládejme, že pro nějaká $0 \leq i < j < n$, $a \in \mathbb{Z}_p^\times$, $b \in \mathbb{Z}_p$ je polynom $ax^j + bx^i$ kódové slovo. Pak $f \mid ax^j + bx^i$, tj. $0 = [ax^j + bx^i]_f = a\alpha^j + b\alpha^i = a\alpha^i(\alpha^{j-i} - b \cdot a^{-1})$. Protože K je těleso a platí $a\alpha^i \neq 0$, plyne odtud $\alpha^{j-i} = b \cdot a^{-1}$. Proto $b \neq 0$, a tedy $b \cdot a^{-1} \in \mathbb{Z}_p^\times$. Z Eulerovy věty víme, že $(p-1)$-tá mocnina libovolného prvku z $\mathbb{Z}_p^\times$ je 1, proto $\alpha^{(j-i)(p-1)} = (b \cdot a^{-1})^{p-1} = 1$.

Kód opravující chybu na jedné pozici

Věta. *Nechť p je prvočíslo a $f \in \mathbb{Z}_p[x]$ je normovaný ireducibilní polynom, $m = \mathrm{st}(f) > 1$. Předpokládejme, že polynom f je zvolen tak, že v tělese $K = \mathbb{Z}_p[x]/[0]_f$ je prvek $\alpha = [x]_f \in K$ generátor multiplikativní grupy $(K^\times, \cdot)$ tělesa K. Pak polynomiální kód délky $n = \frac{p^m-1}{p-1}$ daný polynomem f je schopen opravit chybu na jedné pozici.*

Důkaz. Platí $\mathrm{st}(f) = m < 1 + p + \cdots + p^{m-1} = n$. Stačí ukázat, že žádné kódové slovo nemá vzdálenost 1 nebo 2 od nuly. Sporem: předpokládejme, že pro nějaká $0 \leq i < j < n$, $a \in \mathbb{Z}_p^\times$, $b \in \mathbb{Z}_p$ je polynom $ax^j + bx^i$ kódové slovo. Pak $f \mid ax^j + bx^i$, tj. $0 = [ax^j + bx^i]_f = a\alpha^j + b\alpha^i = a\alpha^i(\alpha^{j-i} - b \cdot a^{-1})$. Protože K je těleso a platí $a\alpha^i \neq 0$, plyne odtud $\alpha^{j-i} = b \cdot a^{-1}$. Proto $b \neq 0$, a tedy $b \cdot a^{-1} \in \mathbb{Z}_p^\times$. Z Eulerovy věty víme, že $(p-1)$-tá mocnina libovolného prvku z $\mathbb{Z}_p^\times$ je 1, proto $\alpha^{(j-i)(p-1)} = (b \cdot a^{-1})^{p-1} = 1$. Protože řád prvku α v grupě $K^\times$ je $p^m - 1$, dostáváme $p^m - 1 \mid (j-i)(p-1)$, tj. $n \mid j - i$, což je ve sporu s tím, že $0 < j - i < n$.

Užití kódu z věty - kódování přehledně

Parametry kódu: p prvočíslo, $m \in \mathbb{N}$, $m > 1$,
$f \in \mathbb{Z}_p[x]$ normovaný, ireducibilní, $\mathrm{st}(f) = m$,
$\alpha = [x]_f$ je generátor grupy $(K^\times, \cdot)$, kde $K = \mathbb{Z}_p[x]/[0]_f$,
$n = \frac{p^m - 1}{p-1} = p^{m-1} + p^{m-2} + \cdots + p + 1$.

Užití kódu z věty - kódování přehledně

Parametry kódu: p prvočíslo, $m \in \mathbb{N}$, $m > 1$,
$f \in \mathbb{Z}_p[x]$ normovaný, ireducibilní, $\mathrm{st}(f) = m$,
$\alpha = [x]_f$ je generátor grupy $(K^\times, \cdot)$, kde $K = \mathbb{Z}_p[x]/[0]_f$,
$n = \frac{p^m - 1}{p-1} = p^{m-1} + p^{m-2} + \cdots + p + 1$.

Nutný předpoklad pro správnou funkci kódu: K chybám při přenosu dochází tak zřídka, že lze očekávat, že při odeslání n písmen (tj. koeficientů odesílaného polynomu) bude nejvýše jedno písmeno přijato chybně.

Užití kódu z věty - kódování přehledně

Parametry kódu: p prvočíslo, $m \in \mathbb{N}$, $m > 1$,
$f \in \mathbb{Z}_p[x]$ normovaný, ireducibilní, $\mathrm{st}(f) = m$,
$\alpha = [x]_f$ je generátor grupy $(K^\times, \cdot)$, kde $K = \mathbb{Z}_p[x]/[0]_f$,
$n = \frac{p^m - 1}{p-1} = p^{m-1} + p^{m-2} + \cdots + p + 1$.

Nutný předpoklad pro správnou funkci kódu: K chybám při přenosu dochází tak zřídka, že lze očekávat, že při odeslání n písmen (tj. koeficientů odesílaného polynomu) bude nejvýše jedno písmeno přijato chybně.

Zpráva určená k odeslání: polynom $b \in \mathbb{Z}_p[x]$, $\mathrm{st}(b) < n - m$,

Užití kódu z věty - kódování přehledně

Parametry kódu: p prvočíslo, $m \in \mathbb{N}$, $m > 1$,
$f \in \mathbb{Z}_p[x]$ normovaný, ireducibilní, $\mathrm{st}(f) = m$,
$\alpha = [x]_f$ je generátor grupy $(K^\times, \cdot)$, kde $K = \mathbb{Z}_p[x]/[0]_f$,
$n = \frac{p^m - 1}{p-1} = p^{m-1} + p^{m-2} + \cdots + p + 1$.

Nutný předpoklad pro správnou funkci kódu: K chybám při přenosu dochází tak zřídka, že lze očekávat, že při odeslání n písmen (tj. koeficientů odesílaného polynomu) bude nejvýše jedno písmeno přijato chybně.

Zpráva určená k odeslání: polynom $b \in \mathbb{Z}_p[x]$, $\mathrm{st}(b) < n - m$,
dělením se zbytkem dostaneme polynomy $q, r \in \mathbb{Z}_p[x]$:
$x^m \cdot b = f \cdot q + r$, kde $\mathrm{st}(r) < m$.

Užití kódu z věty - kódování přehledně

Parametry kódu: p prvočíslo, $m \in \mathbb{N}$, $m > 1$,
$f \in \mathbb{Z}_p[x]$ normovaný, ireducibilní, $\mathrm{st}(f) = m$,
$\alpha = [x]_f$ je generátor grupy $(K^\times, \cdot)$, kde $K = \mathbb{Z}_p[x]/[0]_f$,
$n = \frac{p^m - 1}{p-1} = p^{m-1} + p^{m-2} + \cdots + p + 1$.

Nutný předpoklad pro správnou funkci kódu: K chybám při přenosu dochází tak zřídka, že lze očekávat, že při odeslání n písmen (tj. koeficientů odesílaného polynomu) bude nejvýše jedno písmeno přijato chybně.

Zpráva určená k odeslání: polynom $b \in \mathbb{Z}_p[x]$, $\mathrm{st}(b) < n - m$,
dělením se zbytkem dostaneme polynomy $q, r \in \mathbb{Z}_p[x]$:
$x^m \cdot b = f \cdot q + r$, kde $\mathrm{st}(r) < m$.

Odeslaná informace:
$f \cdot q = x^m \cdot b - r$.

Užití kódu z věty - dekódování přehledně

Parametry kódu: p prvočíslo, $m \in \mathbb{N}$, $m > 1$, $f \in \mathbb{Z}_p[x]$ normovaný, ireducibilní, $\mathrm{st}(f) = m$, $\alpha = [x]_f$ je generátor grupy $(K^\times, \cdot)$, kde $K = \mathbb{Z}_p[x]/[0]_f$, $n = \frac{p^m - 1}{p-1}$.

Přijatá informace: polynom $h \in \mathbb{Z}_p[x]$, $\mathrm{st}(h) < n$.

Užití kódu z věty - dekódování přehledně

Parametry kódu: p prvočíslo, $m \in \mathbb{N}$, $m > 1$, $f \in \mathbb{Z}_p[x]$ normovaný, ireducibilní, $\mathrm{st}(f) = m$, $\alpha = [x]_f$ je generátor grupy $(K^\times, \cdot)$, kde $K = \mathbb{Z}_p[x]/[0]_f$, $n = \frac{p^m - 1}{p-1}$.

Přijatá informace: polynom $h \in \mathbb{Z}_p[x]$, $\mathrm{st}(h) < n$.

Pokud nedošlo při přenosu **k žádné chybě**, byl polynom h odeslán, proto $f \mid h$, tj. $h(\alpha) = 0$.

Užití kódu z věty - dekódování přehledně

Parametry kódu: p prvočíslo, $m \in \mathbb{N}$, $m > 1$, $f \in \mathbb{Z}_p[x]$ normovaný, ireducibilní, $\mathrm{st}(f) = m$, $\alpha = [x]_f$ je generátor grupy $(K^\times, \cdot)$, kde $K = \mathbb{Z}_p[x]/[0]_f$, $n = \frac{p^m - 1}{p-1}$.

Přijatá informace: polynom $h \in \mathbb{Z}_p[x]$, $\mathrm{st}(h) < n$.

Pokud nedošlo při přenosu **k žádné chybě**, byl polynom h odeslán, proto $f \mid h$, tj. $h(\alpha) = 0$.

Pokud došlo při přenosu **k jediné chybě**, byl odeslán polynom $h - cx^j$, kde $c \in \mathbb{Z}_p^\times$, $0 \leq j < n$. Potřebujeme určit c, j.

Užití kódu z věty - dekódování přehledně

Parametry kódu: p prvočíslo, $m \in \mathbb{N}$, $m > 1$, $f \in \mathbb{Z}_p[x]$ normovaný, ireducibilní, $\mathrm{st}(f) = m$, $\alpha = [x]_f$ je generátor grupy $(K^\times, \cdot)$, kde $K = \mathbb{Z}_p[x]/[0]_f$, $n = \frac{p^m - 1}{p-1}$.

Přijatá informace: polynom $h \in \mathbb{Z}_p[x]$, $\mathrm{st}(h) < n$.

Pokud nedošlo při přenosu **k žádné chybě**, byl polynom h odeslán, proto $f \mid h$, tj. $h(\alpha) = 0$.

Pokud došlo při přenosu **k jediné chybě**, byl odeslán polynom $h - cx^j$, kde $c \in \mathbb{Z}_p^\times$, $0 \leq j < n$. Potřebujeme určit c, j. Platí $f \mid h - cx^j$, tedy $0 = [h - cx^j]_f = h(\alpha) - c\alpha^j$, tj. $h(\alpha) = c\alpha^j \neq 0$.

Užití kódu z věty - dekódování přehledně

Parametry kódu: p prvočíslo, $m \in \mathbb{N}$, $m > 1$, $f \in \mathbb{Z}_p[x]$ normovaný, ireducibilní, $\mathrm{st}(f) = m$, $\alpha = [x]_f$ je generátor grupy $(K^\times, \cdot)$, kde $K = \mathbb{Z}_p[x]/[0]_f$, $n = \frac{p^m-1}{p-1}$.

Přijatá informace: polynom $h \in \mathbb{Z}_p[x]$, $\mathrm{st}(h) < n$.

Pokud nedošlo při přenosu **k žádné chybě**, byl polynom h odeslán, proto $f \mid h$, tj. $h(\alpha) = 0$.

Pokud došlo při přenosu **k jediné chybě**, byl odeslán polynom $h - cx^j$, kde $c \in \mathbb{Z}_p^\times$, $0 \leq j < n$. Potřebujeme určit c, j. Platí $f \mid h - cx^j$, tedy $0 = [h - cx^j]_f = h(\alpha) - c\alpha^j$, tj. $h(\alpha) = c\alpha^j \neq 0$. Protože $h(\alpha) \in K^\times = \langle \alpha \rangle$, existuje jediné $t \in \mathbb{Z}$, $0 \leq t < p^m - 1$ splňující $h(\alpha) = \alpha^t$.

Užití kódu z věty - dekódování přehledně

Parametry kódu: p prvočíslo, $m \in \mathbb{N}$, $m > 1$, $f \in \mathbb{Z}_p[x]$ normovaný, ireducibilní, $\mathrm{st}(f) = m$, $\alpha = [x]_f$ je generátor grupy $(K^\times, \cdot)$, kde $K = \mathbb{Z}_p[x]/[0]_f$, $n = \frac{p^m-1}{p-1}$.

Přijatá informace: polynom $h \in \mathbb{Z}_p[x]$, $\mathrm{st}(h) < n$.

Pokud nedošlo při přenosu **k žádné chybě**, byl polynom h odeslán, proto $f \mid h$, tj. $h(\alpha) = 0$.

Pokud došlo při přenosu **k jediné chybě**, byl odeslán polynom $h - cx^j$, kde $c \in \mathbb{Z}_p^\times$, $0 \leq j < n$. Potřebujeme určit c, j. Platí $f \mid h - cx^j$, tedy $0 = [h - cx^j]_f = h(\alpha) - c\alpha^j$, tj. $h(\alpha) = c\alpha^j \neq 0$. Protože $h(\alpha) \in K^\times = \langle \alpha \rangle$, existuje jediné $t \in \mathbb{Z}$, $0 \leq t < p^m - 1$ splňující $h(\alpha) = \alpha^t$. Toto t nalezneme, pak $c = \alpha^{t-j} \in \mathbb{Z}_p^\times$.

Užití kódu z věty - dekódování přehledně

Parametry kódu: p prvočíslo, $m \in \mathbb{N}$, $m > 1$, $f \in \mathbb{Z}_p[x]$ normovaný, ireducibilní, $\mathrm{st}(f) = m$, $\alpha = [x]_f$ je generátor grupy $(K^\times, \cdot)$, kde $K = \mathbb{Z}_p[x]/[0]_f$, $n = \frac{p^m-1}{p-1}$.

Přijatá informace: polynom $h \in \mathbb{Z}_p[x]$, $\mathrm{st}(h) < n$.

Pokud nedošlo při přenosu **k žádné chybě**, byl polynom h odeslán, proto $f \mid h$, tj. $h(\alpha) = 0$.

Pokud došlo při přenosu **k jediné chybě**, byl odeslán polynom $h - cx^j$, kde $c \in \mathbb{Z}_p^\times$, $0 \leq j < n$. Potřebujeme určit c, j. Platí $f \mid h - cx^j$, tedy $0 = [h - cx^j]_f = h(\alpha) - c\alpha^j$, tj. $h(\alpha) = c\alpha^j \neq 0$. Protože $h(\alpha) \in K^\times = \langle \alpha \rangle$, existuje jediné $t \in \mathbb{Z}$, $0 \leq t < p^m - 1$ splňující $h(\alpha) = \alpha^t$. Toto t nalezneme, pak $c = \alpha^{t-j} \in \mathbb{Z}_p^\times$.
Z Eulerovy věty $1 = c^{p-1} = \alpha^{(t-j)(p-1)}$.

Užití kódu z věty - dekódování přehledně

Parametry kódu: p prvočíslo, $m \in \mathbb{N}$, $m > 1$, $f \in \mathbb{Z}_p[x]$ normovaný, ireducibilní, $\mathrm{st}(f) = m$, $\alpha = [x]_f$ je generátor grupy $(K^\times, \cdot)$, kde $K = \mathbb{Z}_p[x]/[0]_f$, $n = \frac{p^m-1}{p-1}$.

Přijatá informace: polynom $h \in \mathbb{Z}_p[x]$, $\mathrm{st}(h) < n$.

Pokud nedošlo při přenosu **k žádné chybě**, byl polynom h odeslán, proto $f \mid h$, tj. $h(\alpha) = 0$.

Pokud došlo při přenosu **k jediné chybě**, byl odeslán polynom $h - cx^j$, kde $c \in \mathbb{Z}_p^\times$, $0 \leq j < n$. Potřebujeme určit c, j. Platí $f \mid h - cx^j$, tedy $0 = [h - cx^j]_f = h(\alpha) - c\alpha^j$, tj. $h(\alpha) = c\alpha^j \neq 0$. Protože $h(\alpha) \in K^\times = \langle \alpha \rangle$, existuje jediné $t \in \mathbb{Z}$, $0 \leq t < p^m - 1$ splňující $h(\alpha) = \alpha^t$. Toto t nalezneme, pak $c = \alpha^{t-j} \in \mathbb{Z}_p^\times$.
Z Eulerovy věty $1 = c^{p-1} = \alpha^{(t-j)(p-1)}$. Protože řád α je $p^m - 1$, platí $p^m - 1 \mid (t-j)(p-1)$, tj. $n = \frac{p^m-1}{p-1} \mid t - j$.

Užití kódu z věty - dekódování přehledně

Parametry kódu: p prvočíslo, $m \in \mathbb{N}$, $m > 1$, $f \in \mathbb{Z}_p[x]$ normovaný, ireducibilní, $\mathrm{st}(f) = m$, $\alpha = [x]_f$ je generátor grupy $(K^\times, \cdot)$, kde $K = \mathbb{Z}_p[x]/[0]_f$, $n = \frac{p^m-1}{p-1}$.

Přijatá informace: polynom $h \in \mathbb{Z}_p[x]$, $\mathrm{st}(h) < n$.

Pokud nedošlo při přenosu **k žádné chybě**, byl polynom h odeslán, proto $f \mid h$, tj. $h(\alpha) = 0$.

Pokud došlo při přenosu **k jediné chybě**, byl odeslán polynom $h - cx^j$, kde $c \in \mathbb{Z}_p^\times$, $0 \leq j < n$. Potřebujeme určit c, j. Platí $f \mid h - cx^j$, tedy $0 = [h - cx^j]_f = h(\alpha) - c\alpha^j$, tj. $h(\alpha) = c\alpha^j \neq 0$. Protože $h(\alpha) \in K^\times = \langle \alpha \rangle$, existuje jediné $t \in \mathbb{Z}$, $0 \leq t < p^m - 1$ splňující $h(\alpha) = \alpha^t$. Toto t nalezneme, pak $c = \alpha^{t-j} \in \mathbb{Z}_p^\times$.
Z Eulerovy věty $1 = c^{p-1} = \alpha^{(t-j)(p-1)}$. Protože řád α je $p^m - 1$, platí $p^m - 1 \mid (t-j)(p-1)$, tj. $n = \frac{p^m-1}{p-1} \mid t - j$. Číslo j nalezneme jako zbytek po dělení čísla t číslem n a víme, že $c = \alpha^{t-j} \in \mathbb{Z}_p^\times$.

Užití kódu z věty - dekódování přehledně

Parametry kódu: p prvočíslo, $m \in \mathbb{N}$, $m > 1$, $f \in \mathbb{Z}_p[x]$ normovaný, ireducibilní, $\mathrm{st}(f) = m$, $\alpha = [x]_f$ je generátor grupy $(K^\times, \cdot)$, kde $K = \mathbb{Z}_p[x]/[0]_f$, $n = \frac{p^m-1}{p-1}$.

Přijatá informace: polynom $h \in \mathbb{Z}_p[x]$, $\mathrm{st}(h) < n$.

Pokud nedošlo při přenosu **k žádné chybě**, byl polynom h odeslán, proto $f \mid h$, tj. $h(\alpha) = 0$.

Pokud došlo při přenosu **k jediné chybě**, byl odeslán polynom $h - cx^j$, kde $c \in \mathbb{Z}_p^\times$, $0 \leq j < n$. Potřebujeme určit c, j. Platí $f \mid h - cx^j$, tedy $0 = [h - cx^j]_f = h(\alpha) - c\alpha^j$, tj. $h(\alpha) = c\alpha^j \neq 0$. Protože $h(\alpha) \in K^\times = \langle\alpha\rangle$, existuje jediné $t \in \mathbb{Z}$, $0 \leq t < p^m - 1$ splňující $h(\alpha) = \alpha^t$. Toto t nalezneme, pak $c = \alpha^{t-j} \in \mathbb{Z}_p^\times$.
Z Eulerovy věty $1 = c^{p-1} = \alpha^{(t-j)(p-1)}$. Protože řád α je $p^m - 1$, platí $p^m - 1 \mid (t-j)(p-1)$, tj. $n = \frac{p^m-1}{p-1} \mid t - j$. Číslo j nalezneme jako zbytek po dělení čísla t číslem n a víme, že $c = \alpha^{t-j} \in \mathbb{Z}_p^\times$.

Odeslaný polynom: je-li $h(\alpha) = 0$, byl odeslán h; je-li $h(\alpha) \neq 0$, byl odeslán $h - cx^j$ (pro výše určené c, j).

Příklad kódu opravujícího chybu na jedné pozici

Zvolme $p = 2$ a $m = 3$, pak $n = 7$.

Příklad kódu opravujícího chybu na jedné pozici

Zvolme $p = 2$ a $m = 3$, pak $n = 7$. Podmínku věty splňuje polynom $f = x^3 + x + 1$.

Příklad kódu opravujícího chybu na jedné pozici

Zvolme $p = 2$ a $m = 3$, pak $n = 7$. Podmínku věty splňuje polynom $f = x^3 + x + 1$. Vzniklý kód má 4 významová a 3 kontrolní písmena.

Příklad kódu opravujícího chybu na jedné pozici

Zvolme $p = 2$ a $m = 3$, pak $n = 7$. Podmínku věty splňuje polynom $f = x^3 + x + 1$. Vzniklý kód má 4 významová a 3 kontrolní písmena.

Zprávou je čtveřice $(a, b, c, d) \in \mathbb{Z}_2^4$, což jsou koeficienty polynomu $ax^3 + bx^2 + cx + d$.

Příklad kódu opravujícího chybu na jedné pozici

Zvolme $p = 2$ a $m = 3$, pak $n = 7$. Podmínku věty splňuje polynom $f = x^3 + x + 1$. Vzniklý kód má 4 významová a 3 kontrolní písmena.

Zprávou je čtveřice $(a, b, c, d) \in \mathbb{Z}_2^4$, což jsou koeficienty polynomu $ax^3 + bx^2 + cx + d$. Dělením se zbytkem v $\mathbb{Z}_2[x]$ dostaneme

$$(ax^3 + bx^2 + cx + d) \cdot x^3 = (ax^3 + bx^2 + (a+c)x + (a+b+d)) \cdot f + \\ + (a + b + c)x^2 + (b + c + d)x + (a + b + d).$$

Příklad kódu opravujícího chybu na jedné pozici

Zvolme $p = 2$ a $m = 3$, pak $n = 7$. Podmínku věty splňuje polynom $f = x^3 + x + 1$. Vzniklý kód má 4 významová a 3 kontrolní písmena.

Zprávou je čtveřice $(a, b, c, d) \in \mathbb{Z}_2^4$, což jsou koeficienty polynomu $ax^3 + bx^2 + cx + d$. Dělením se zbytkem v $\mathbb{Z}_2[x]$ dostaneme

$$(ax^3 + bx^2 + cx + d) \cdot x^3 = (ax^3 + bx^2 + (a+c)x + (a+b+d)) \cdot f + \\ + (a + b + c)x^2 + (b + c + d)x + (a + b + d).$$

Odesíláme polynom $ax^6 + bx^5 + cx^4 + dx^3 + ux^2 + vx + w$,kde $u = a + b + c$, $v = b + c + d$, $w = a + b + d$.

Příklad kódu opravujícího chybu na jedné pozici

Zvolme $p = 2$ a $m = 3$, pak $n = 7$. Podmínku věty splňuje polynom $f = x^3 + x + 1$. Vzniklý kód má 4 významová a 3 kontrolní písmena.

Zprávou je čtveřice $(a, b, c, d) \in \mathbb{Z}_2^4$, což jsou koeficienty polynomu $ax^3 + bx^2 + cx + d$. Dělením se zbytkem v $\mathbb{Z}_2[x]$ dostaneme

$$(ax^3 + bx^2 + cx + d) \cdot x^3 = (ax^3 + bx^2 + (a+c)x + (a+b+d)) \cdot f + \\ + (a + b + c)x^2 + (b + c + d)x + (a + b + d).$$

Odesíláme polynom $ax^6 + bx^5 + cx^4 + dx^3 + ux^2 + vx + w$,kde $u = a + b + c$, $v = b + c + d$, $w = a + b + d$. Tento polynom je dělitelný polynomem f.

Příklad kódu opravujícího chybu na jedné pozici

Zvolme $p = 2$ a $m = 3$, pak $n = 7$. Podmínku věty splňuje polynom $f = x^3 + x + 1$. Vzniklý kód má 4 významová a 3 kontrolní písmena.

Zprávou je čtveřice $(a, b, c, d) \in \mathbb{Z}_2^4$, což jsou koeficienty polynomu $ax^3 + bx^2 + cx + d$. Dělením se zbytkem v $\mathbb{Z}_2[x]$ dostaneme

$$(ax^3 + bx^2 + cx + d) \cdot x^3 = (ax^3 + bx^2 + (a+c)x + (a+b+d)) \cdot f + \\ + (a + b + c)x^2 + (b + c + d)x + (a + b + d).$$

Odesíláme polynom $ax^6 + bx^5 + cx^4 + dx^3 + ux^2 + vx + w$,kde $u = a + b + c$, $v = b + c + d$, $w = a + b + d$. Tento polynom je dělitelný polynomem f.

Přijatým polynomem je $h \in \mathbb{Z}_2[x]$, $\mathrm{st}(h) < 7$.

Příklad kódu opravujícího chybu na jedné pozici

Zvolme $p = 2$ a $m = 3$, pak $n = 7$. Podmínku věty splňuje polynom $f = x^3 + x + 1$. Vzniklý kód má 4 významová a 3 kontrolní písmena.

Zprávou je čtveřice $(a, b, c, d) \in \mathbb{Z}_2^4$, což jsou koeficienty polynomu $ax^3 + bx^2 + cx + d$. Dělením se zbytkem v $\mathbb{Z}_2[x]$ dostaneme

$$(ax^3 + bx^2 + cx + d) \cdot x^3 = (ax^3 + bx^2 + (a+c)x + (a+b+d)) \cdot f + \\ + (a + b + c)x^2 + (b + c + d)x + (a + b + d).$$

Odesíláme polynom $ax^6 + bx^5 + cx^4 + dx^3 + ux^2 + vx + w$,kde $u = a + b + c$, $v = b + c + d$, $w = a + b + d$. Tento polynom je dělitelný polynomem f.

Přijatým polynomem je $h \in \mathbb{Z}_2[x]$, $\mathrm{st}(h) < 7$. Nedošlo-li k žádné chybě, platí $f \mid h$ v $\mathbb{Z}_p[x]$, tj. $h(\alpha) = 0$.

Příklad kódu opravujícího chybu na jedné pozici

Zvolme $p = 2$ a $m = 3$, pak $n = 7$. Podmínku věty splňuje polynom $f = x^3 + x + 1$. Vzniklý kód má 4 významová a 3 kontrolní písmena.

Zprávou je čtveřice $(a, b, c, d) \in \mathbb{Z}_2^4$, což jsou koeficienty polynomu $ax^3 + bx^2 + cx + d$. Dělením se zbytkem v $\mathbb{Z}_2[x]$ dostaneme

$$(ax^3 + bx^2 + cx + d) \cdot x^3 = (ax^3 + bx^2 + (a+c)x + (a+b+d)) \cdot f + \\ + (a + b + c)x^2 + (b + c + d)x + (a + b + d).$$

Odesíláme polynom $ax^6 + bx^5 + cx^4 + dx^3 + ux^2 + vx + w$,kde $u = a + b + c$, $v = b + c + d$, $w = a + b + d$. Tento polynom je dělitelný polynomem f.

Přijatým polynomem je $h \in \mathbb{Z}_2[x]$, $\mathrm{st}(h) < 7$. Nedošlo-li k žádné chybě, platí $f \mid h$ v $\mathbb{Z}_p[x]$, tj. $h(\alpha) = 0$. Došlo-li k jediné chybě, byl odesílán polynom $h - x^e$ pro nějaké $0 \leq e < 7$ a platí $\alpha^e = h(\alpha)$.

Příklad kódu opravujícího chybu na jedné pozici

Zvolme $p = 2$ a $m = 3$, pak $n = 7$. Podmínku věty splňuje polynom $f = x^3 + x + 1$. Vzniklý kód má 4 významová a 3 kontrolní písmena.

Zprávou je čtveřice $(a, b, c, d) \in \mathbb{Z}_2^4$, což jsou koeficienty polynomu $ax^3 + bx^2 + cx + d$. Dělením se zbytkem v $\mathbb{Z}_2[x]$ dostaneme

$$(ax^3 + bx^2 + cx + d) \cdot x^3 = (ax^3 + bx^2 + (a+c)x + (a+b+d)) \cdot f + \\ + (a + b + c)x^2 + (b + c + d)x + (a + b + d).$$

Odesíláme polynom $ax^6 + bx^5 + cx^4 + dx^3 + ux^2 + vx + w$,kde $u = a + b + c$, $v = b + c + d$, $w = a + b + d$. Tento polynom je dělitelný polynomem f.

Přijatým polynomem je $h \in \mathbb{Z}_2[x]$, $\mathrm{st}(h) < 7$. Nedošlo-li k žádné chybě, platí $f \mid h$ v $\mathbb{Z}_p[x]$, tj. $h(\alpha) = 0$. Došlo-li k jediné chybě, byl odesílán polynom $h - x^e$ pro nějaké $0 \leq e < 7$ a platí $\alpha^e = h(\alpha)$. Odpovídající e zjistíme z tabulky pro vypočtené $h(\alpha)$:

$e = 0$	1	$e = 2$	α^2	$e = 4$	$\alpha^2 + \alpha$	$e = 6$	$\alpha^2 + 1$
$e = 1$	α	$e = 3$	$\alpha + 1$	$e = 5$	$\alpha^2 + \alpha + 1$		

Příklad kódu opravujícího chybu na jedné pozici

Zvolme $p = 2$ a $m = 3$, pak $n = 7$. Podmínku věty splňuje polynom $f = x^3 + x + 1$. Vzniklý kód má 4 významová a 3 kontrolní písmena.

Zprávou je čtveřice $(a, b, c, d) \in \mathbb{Z}_2^4$, což jsou koeficienty polynomu $ax^3 + bx^2 + cx + d$. Dělením se zbytkem v $\mathbb{Z}_2[x]$ dostaneme

$$(ax^3 + bx^2 + cx + d) \cdot x^3 = (ax^3 + bx^2 + (a+c)x + (a+b+d)) \cdot f + \\ + (a + b + c)x^2 + (b + c + d)x + (a + b + d).$$

Odesíláme polynom $ax^6 + bx^5 + cx^4 + dx^3 + ux^2 + vx + w$,kde $u = a + b + c$, $v = b + c + d$, $w = a + b + d$. Tento polynom je dělitelný polynomem f.

Přijatým polynomem je $h \in \mathbb{Z}_2[x]$, $\mathrm{st}(h) < 7$. Nedošlo-li k žádné chybě, platí $f \mid h$ v $\mathbb{Z}_p[x]$, tj. $h(\alpha) = 0$. Došlo-li k jediné chybě, byl odesílán polynom $h - x^e$ pro nějaké $0 \leq e < 7$ a platí $\alpha^e = h(\alpha)$. Odpovídající e zjistíme z tabulky pro vypočtené $h(\alpha)$:

$e = 0$	1	$e = 2$	α^2	$e = 4$	$\alpha^2 + \alpha$	$e = 6$	$\alpha^2 + 1$
$e = 1$	α	$e = 3$	$\alpha + 1$	$e = 5$	$\alpha^2 + \alpha + 1$		

Pokud došlo k více než jedné chybě, vyhodnotíme přijatý polynom špatně (chybu vůbec nezjistíme, anebo ji špatně opravíme).

Kód Reed–Solomon opravující chyby na více pozicích

Věta. *Nechť p je prvočíslo a $f \in \mathbb{Z}_p[x]$ je normovaný ireducibilní polynom, $m = \mathrm{st}(f) > 1$.*

Kód Reed–Solomon opravující chyby na více pozicích

Věta. *Nechť p je prvočíslo a $f \in \mathbb{Z}_p[x]$ je normovaný ireducibilní polynom, $m = \mathrm{st}(f) > 1$. Předpokládejme, že polynom f je zvolen tak, že v tělese $K = \mathbb{Z}_p[x]/[0]_f$ prvek $\alpha = [x]_f \in K$ je generátor multiplikativní grupy $(K^\times, \cdot)$ tělesa K.*

Kód Reed–Solomon opravující chyby na více pozicích

Věta. *Nechť p je prvočíslo a $f \in \mathbb{Z}_p[x]$ je normovaný ireducibilní polynom, $m = \mathrm{st}(f) > 1$. Předpokládejme, že polynom f je zvolen tak, že v tělese $K = \mathbb{Z}_p[x]/[0]_f$ prvek $\alpha = [x]_f \in K$ je generátor multiplikativní grupy $(K^\times, \cdot)$ tělesa K. Nechť $r, t \in \mathbb{Z}$, $r \geq -1$, $0 < t < p^m - 1$.*

Kód Reed–Solomon opravující chyby na více pozicích

Věta. *Nechť p je prvočíslo a $f \in \mathbb{Z}_p[x]$ je normovaný ireducibilní polynom, $m = \mathrm{st}(f) > 1$. Předpokládejme, že polynom f je zvolen tak, že v tělese $K = \mathbb{Z}_p[x]/[0]_f$ prvek $\alpha = [x]_f \in K$ je generátor multiplikativní grupy $(K^\times, \cdot)$ tělesa K. Nechť $r, t \in \mathbb{Z}$, $r \geq -1$, $0 < t < p^m - 1$. Předpokládejme, že pro polynom $g \in \mathbb{Z}_p[x]$ platí $\mathrm{st}(g) < p^m - 1$ a $g(\alpha^{r+j}) = 0$ pro každé $j = 1, 2, \ldots, 2t$.*

Kód Reed–Solomon opravující chyby na více pozicích

Věta. *Nechť p je prvočíslo a $f \in \mathbb{Z}_p[x]$ je normovaný ireducibilní polynom, $m = \mathrm{st}(f) > 1$. Předpokládejme, že polynom f je zvolen tak, že v tělese $K = \mathbb{Z}_p[x]/[0]_f$ prvek $\alpha = [x]_f \in K$ je generátor multiplikativní grupy $(K^\times, \cdot)$ tělesa K. Nechť $r, t \in \mathbb{Z}$, $r \geq -1$, $0 < t < p^m - 1$. Předpokládejme, že pro polynom $g \in \mathbb{Z}_p[x]$ platí $\mathrm{st}(g) < p^m - 1$ a $g(\alpha^{r+j}) = 0$ pro každé $j = 1, 2, \ldots, 2t$. Pak polynomiální kód délky $n = p^m - 1$ daný polynomem g je schopen opravit chybu na t pozicích.*

Kód Reed–Solomon opravující chyby na více pozicích

Věta. *Nechť p je prvočíslo a $f \in \mathbb{Z}_p[x]$ je normovaný ireducibilní polynom, $m = \mathrm{st}(f) > 1$. Předpokládejme, že polynom f je zvolen tak, že v tělese $K = \mathbb{Z}_p[x]/[0]_f$ prvek $\alpha = [x]_f \in K$ je generátor multiplikativní grupy $(K^\times, \cdot)$ tělesa K. Nechť $r, t \in \mathbb{Z}$, $r \geq -1$, $0 < t < p^m - 1$. Předpokládejme, že pro polynom $g \in \mathbb{Z}_p[x]$ platí $\mathrm{st}(g) < p^m - 1$ a $g(\alpha^{r+j}) = 0$ pro každé $j = 1, 2, \ldots, 2t$. Pak polynomiální kód délky $n = p^m - 1$ daný polynomem g je schopen opravit chybu na t pozicích.*

Důkaz. Předpokládejme, že existuje nenulové kódové slovo, jehož vzdálenost od nuly nepřevyšuje $2t$.

Kód Reed–Solomon opravující chyby na více pozicích

Věta. *Nechť p je prvočíslo a $f \in \mathbb{Z}_p[x]$ je normovaný ireducibilní polynom, $m = \mathrm{st}(f) > 1$. Předpokládejme, že polynom f je zvolen tak, že v tělese $K = \mathbb{Z}_p[x]/[0]_f$ prvek $\alpha = [x]_f \in K$ je generátor multiplikativní grupy $(K^\times, \cdot)$ tělesa K. Nechť $r, t \in \mathbb{Z}$, $r \geq -1$, $0 < t < p^m - 1$. Předpokládejme, že pro polynom $g \in \mathbb{Z}_p[x]$ platí $\mathrm{st}(g) < p^m - 1$ a $g(\alpha^{r+j}) = 0$ pro každé $j = 1, 2, \ldots, 2t$. Pak polynomiální kód délky $n = p^m - 1$ daný polynomem g je schopen opravit chybu na t pozicích.*

Důkaz. Předpokládejme, že existuje nenulové kódové slovo, jehož vzdálenost od nuly nepřevyšuje $2t$. Existují tedy $b_1, \ldots, b_{2t} \in \mathbb{Z}_p$, ne všechny nuly, a $0 \leq k_1 < k_2 < \cdots < k_{2t} < n$ tak, že polynom $h = \sum_{i=1}^{2t} b_i x^{k_i}$ je kódové slovo, tj. $g \mid h$,

Kód Reed–Solomon opravující chyby na více pozicích

Věta. *Nechť p je prvočíslo a $f \in \mathbb{Z}_p[x]$ je normovaný ireducibilní polynom, $m = \mathrm{st}(f) > 1$. Předpokládejme, že polynom f je zvolen tak, že v tělese $K = \mathbb{Z}_p[x]/[0]_f$ prvek $\alpha = [x]_f \in K$ je generátor multiplikativní grupy $(K^\times, \cdot)$ tělesa K. Nechť $r, t \in \mathbb{Z}$, $r \geq -1$, $0 < t < p^m - 1$. Předpokládejme, že pro polynom $g \in \mathbb{Z}_p[x]$ platí $\mathrm{st}(g) < p^m - 1$ a $g(\alpha^{r+j}) = 0$ pro každé $j = 1, 2, \ldots, 2t$. Pak polynomiální kód délky $n = p^m - 1$ daný polynomem g je schopen opravit chybu na t pozicích.*

Důkaz. Předpokládejme, že existuje nenulové kódové slovo, jehož vzdálenost od nuly nepřevyšuje $2t$. Existují tedy $b_1, \ldots, b_{2t} \in \mathbb{Z}_p$, ne všechny nuly, a $0 \leq k_1 < k_2 < \cdots < k_{2t} < n$ tak, že polynom $h = \sum_{i=1}^{2t} b_i x^{k_i}$ je kódové slovo, tj. $g \mid h$, a proto $h(\alpha^{r+j}) = 0$ pro každé $j = 1, 2, \ldots, 2t$.

Kód Reed–Solomon opravující chyby na více pozicích

Věta. *Nechť p je prvočíslo a $f \in \mathbb{Z}_p[x]$ je normovaný ireducibilní polynom, $m = \mathrm{st}(f) > 1$. Předpokládejme, že polynom f je zvolen tak, že v tělese $K = \mathbb{Z}_p[x]/[0]_f$ prvek $\alpha = [x]_f \in K$ je generátor multiplikativní grupy $(K^\times, \cdot)$ tělesa K. Nechť $r, t \in \mathbb{Z}$, $r \geq -1$, $0 < t < p^m - 1$. Předpokládejme, že pro polynom $g \in \mathbb{Z}_p[x]$ platí $\mathrm{st}(g) < p^m - 1$ a $g(\alpha^{r+j}) = 0$ pro každé $j = 1, 2, \ldots, 2t$. Pak polynomiální kód délky $n = p^m - 1$ daný polynomem g je schopen opravit chybu na t pozicích.*

Důkaz. Předpokládejme, že existuje nenulové kódové slovo, jehož vzdálenost od nuly nepřevyšuje $2t$. Existují tedy $b_1, \ldots, b_{2t} \in \mathbb{Z}_p$, ne všechny nuly, a $0 \leq k_1 < k_2 < \cdots < k_{2t} < n$ tak, že polynom $h = \sum_{i=1}^{2t} b_i x^{k_i}$ je kódové slovo, tj. $g \mid h$, a proto $h(\alpha^{r+j}) = 0$ pro každé $j = 1, 2, \ldots, 2t$. Pak $(\alpha^{(r+j)k_i})_{j,i=1,2,\ldots,2t}$ je matice s lineárně závislými sloupci.

Kód Reed–Solomon opravující chyby na více pozicích

Věta. *Nechť p je prvočíslo a $f \in \mathbb{Z}_p[x]$ je normovaný ireducibilní polynom, $m = \mathrm{st}(f) > 1$. Předpokládejme, že polynom f je zvolen tak, že v tělese $K = \mathbb{Z}_p[x]/[0]_f$ prvek $\alpha = [x]_f \in K$ je generátor multiplikativní grupy $(K^\times, \cdot)$ tělesa K. Nechť $r, t \in \mathbb{Z}$, $r \geq -1$, $0 < t < p^m - 1$. Předpokládejme, že pro polynom $g \in \mathbb{Z}_p[x]$ platí $\mathrm{st}(g) < p^m - 1$ a $g(\alpha^{r+j}) = 0$ pro každé $j = 1, 2, \ldots, 2t$. Pak polynomiální kód délky $n = p^m - 1$ daný polynomem g je schopen opravit chybu na t pozicích.*

Důkaz. Předpokládejme, že existuje nenulové kódové slovo, jehož vzdálenost od nuly nepřevyšuje $2t$. Existují tedy $b_1, \ldots, b_{2t} \in \mathbb{Z}_p$, ne všechny nuly, a $0 \leq k_1 < k_2 < \cdots < k_{2t} < n$ tak, že polynom $h = \sum_{i=1}^{2t} b_i x^{k_i}$ je kódové slovo, tj. $g \mid h$, a proto $h(\alpha^{r+j}) = 0$ pro každé $j = 1, 2, \ldots, 2t$. Pak $(\alpha^{(r+j)k_i})_{j,i=1,2,\ldots,2t}$ je matice s lineárně závislými sloupci. Ovšem pro $k = \sum_{i=1}^{2t} k_i$ platí $0 = \det(\alpha^{(r+j)k_i})_{j,i=1,2,\ldots,2t} = \alpha^{(r+1)k} \cdot \prod_{1 \leq i < j \leq 2t} (\alpha^{k_j} - \alpha^{k_i})$ užitím vzorce pro Vandermondův determinant.

Kód Reed–Solomon opravující chyby na více pozicích

Věta. *Nechť p je prvočíslo a $f \in \mathbb{Z}_p[x]$ je normovaný ireducibilní polynom, $m = \mathrm{st}(f) > 1$. Předpokládejme, že polynom f je zvolen tak, že v tělese $K = \mathbb{Z}_p[x]/[0]_f$ prvek $\alpha = [x]_f \in K$ je generátor multiplikativní grupy $(K^\times, \cdot)$ tělesa K. Nechť $r, t \in \mathbb{Z}$, $r \geq -1$, $0 < t < p^m - 1$. Předpokládejme, že pro polynom $g \in \mathbb{Z}_p[x]$ platí $\mathrm{st}(g) < p^m - 1$ a $g(\alpha^{r+j}) = 0$ pro každé $j = 1, 2, \ldots, 2t$. Pak polynomiální kód délky $n = p^m - 1$ daný polynomem g je schopen opravit chybu na t pozicích.*

Důkaz. Předpokládejme, že existuje nenulové kódové slovo, jehož vzdálenost od nuly nepřevyšuje $2t$. Existují tedy $b_1, \ldots, b_{2t} \in \mathbb{Z}_p$, ne všechny nuly, a $0 \leq k_1 < k_2 < \cdots < k_{2t} < n$ tak, že polynom $h = \sum_{i=1}^{2t} b_i x^{k_i}$ je kódové slovo, tj. $g \mid h$, a proto $h(\alpha^{r+j}) = 0$ pro každé $j = 1, 2, \ldots, 2t$. Pak $(\alpha^{(r+j)k_i})_{j,i=1,2,\ldots,2t}$ je matice s lineárně závislými sloupci. Ovšem pro $k = \sum_{i=1}^{2t} k_i$ platí $0 = \det(\alpha^{(r+j)k_i})_{j,i=1,2,\ldots,2t} = \alpha^{(r+1)k} \cdot \prod_{1 \leq i < j \leq 2t} (\alpha^{k_j} - \alpha^{k_i})$ užitím vzorce pro Vandermondův determinant. Ale to je součin mající pouze nenulové činitele, neboť α má řád n, spor.

Příklad kódu opravujícího chyby na více pozicích

Polynom $f = x^4 + x + 1 \in \mathbb{Z}_2[x]$ je ireducibilní nad $\mathbb{Z}_2$.

Příklad kódu opravujícího chyby na více pozicích

Polynom $f = x^4 + x + 1 \in \mathbb{Z}_2[x]$ je ireducibilní nad $\mathbb{Z}_2$.
Těleso $K = \mathbb{Z}_2[x]/[x]_f$ má 16 prvků, prvek $\alpha = [x]_f$ generuje multiplikativní grupu $(K^\times, \cdot)$.

Příklad kódu opravujícího chyby na více pozicích

Polynom $f = x^4 + x + 1 \in \mathbb{Z}_2[x]$ je ireducibilní nad $\mathbb{Z}_2$.
Těleso $K = \mathbb{Z}_2[x]/[x]_f$ má 16 prvků, prvek $\alpha = [x]_f$ generuje multiplikativní grupu $(K^\times, \cdot)$.
Polynom $x^4 + x + 1$ má v K kořeny $\alpha, \alpha^2, \alpha^4, \alpha^8$.

Příklad kódu opravujícího chyby na více pozicích

Polynom $f = x^4 + x + 1 \in \mathbb{Z}_2[x]$ je ireducibilní nad $\mathbb{Z}_2$.
Těleso $K = \mathbb{Z}_2[x]/[x]_f$ má 16 prvků, prvek $\alpha = [x]_f$ generuje multiplikativní grupu $(K^\times, \cdot)$.
Polynom $x^4 + x + 1$ má v K kořeny $\alpha, \alpha^2, \alpha^4, \alpha^8$.
Polynom $x^4 + x^3 + x^2 + x + 1$ má v K kořeny $\alpha^3, \alpha^6, \alpha^9, \alpha^{12}$.

Příklad kódu opravujícího chyby na více pozicích

Polynom $f = x^4 + x + 1 \in \mathbb{Z}_2[x]$ je ireducibilní nad $\mathbb{Z}_2$.
Těleso $K = \mathbb{Z}_2[x]/[x]_f$ má 16 prvků, prvek $\alpha = [x]_f$ generuje multiplikativní grupu $(K^\times, \cdot)$.
Polynom $x^4 + x + 1$ má v K kořeny $\alpha, \alpha^2, \alpha^4, \alpha^8$.
Polynom $x^4 + x^3 + x^2 + x + 1$ má v K kořeny $\alpha^3, \alpha^6, \alpha^9, \alpha^{12}$.
Polynom $x^2 + x + 1$ má v K kořeny α^5, α^{10}.

Příklad kódu opravujícího chyby na více pozicích

Polynom $f = x^4 + x + 1 \in \mathbb{Z}_2[x]$ je ireducibilní nad $\mathbb{Z}_2$.
Těleso $K = \mathbb{Z}_2[x]/[x]_f$ má 16 prvků, prvek $\alpha = [x]_f$ generuje multiplikativní grupu $(K^\times, \cdot)$.
Polynom $x^4 + x + 1$ má v K kořeny $\alpha, \alpha^2, \alpha^4, \alpha^8$.
Polynom $x^4 + x^3 + x^2 + x + 1$ má v K kořeny $\alpha^3, \alpha^6, \alpha^9, \alpha^{12}$.
Polynom $x^2 + x + 1$ má v K kořeny α^5, α^{10}.
Proto polynom

$$g = (x^4 + x + 1) \cdot (x^4 + x^3 + x^2 + x + 1) \cdot (x^2 + x + 1) =$$
$$= x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1$$

splňuje předpoklady předchozí věty pro $p = 2$, $m = 4$, $n = 15$, $r = 0$, $t = 3$.

Příklad kódu opravujícího chyby na více pozicích

Polynom $f = x^4 + x + 1 \in \mathbb{Z}_2[x]$ je ireducibilní nad $\mathbb{Z}_2$.
Těleso $K = \mathbb{Z}_2[x]/[x]_f$ má 16 prvků, prvek $\alpha = [x]_f$ generuje multiplikativní grupu $(K^\times, \cdot)$.
Polynom $x^4 + x + 1$ má v K kořeny $\alpha, \alpha^2, \alpha^4, \alpha^8$.
Polynom $x^4 + x^3 + x^2 + x + 1$ má v K kořeny $\alpha^3, \alpha^6, \alpha^9, \alpha^{12}$.
Polynom $x^2 + x + 1$ má v K kořeny α^5, α^{10}.
Proto polynom

$$g = (x^4 + x + 1) \cdot (x^4 + x^3 + x^2 + x + 1) \cdot (x^2 + x + 1) =$$
$$= x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1$$

splňuje předpoklady předchozí věty pro $p = 2$, $m = 4$, $n = 15$, $r = 0$, $t = 3$.
Odpovídající kód délky 15 má 5 významových a 10 kontrolních písmen. Je schopen opravit chyby až na třech pozicích.