ZÁPADOČESKÁ UNIVERZITA V PLZNI
FAKULTA PEDAGOGICKÁ
Katedra matematiky, fyziky a technické výchovy

Jedno užití polynomů nad konečnými tělesy

DIPLOMOVÁ PRÁCE

Bc. Jiří Jandl

Učitelství pro druhý stupeň základní školy, obor Učitelství matematiky a fyziky

Vedoucí práce: doc. RNDr. Jaroslav HORA, CSc.

Plzeň, 2017

Prohlašuji, že jsem diplomovou práci vypracoval samostatně s použitím uvedené literatury a zdrojů informací.

Plzeň, 30. června 2017

.....

vlastnoruční podpis

Děkuji mému vedoucímu diplomové práce doc. RNDr. Jaroslavovi Horovi, CSc., za jeho cenné rady, připomínky a metodické vedení práce.

ZÁPADOČESKÁ UNIVERZITA V PLZNI
Fakulta pedagogická
Akademický rok: **2015/2016**

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Jiří JANDL**
Osobní číslo:	**P15N0064P**
Studijní program:	**N7503 Učitelství pro základní školy**
Studijní obory:	**Učitelství fyziky pro základní školy**
	Učitelství matematiky pro základní školy
Název tématu:	**Jedno užití polynomů nad konečnými tělesy**
Zadávající katedra:	**Katedra matematiky, fyziky a technické výchovy**

Zásady pro vypracování:

Konečná tělesa.
Polynomy nad konečnými tělesy.
Hledání minimálních polynomů prvků konečných těles.
Lineární kódy.
Hammingův kód.
Příklady užití samoopravných kódů.

Rozsah grafických prací:

Rozsah kvalifikační práce: **40 - 60**

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

Bican, L. Algebra II. Skriptum MFF UK Praha. Praha: SPN, 1982.
Gathen, J., Bernard, J. Modern Computer Algebra.
Cambridge University Press, 2003.
Lidl, R., Niederreiter, H. Introduction to finite
fields and their applications. Cambridge University Press,
revidované vydání, 1997.
Procházka, L. a kol. Algebra. Praha: Academia, 1990.
Další knižní a časopisecké prameny, zdroje na internetu,
manuál k počítačovému programu Mathematica.

Vedoucí diplomové práce: **Doc. RNDr. Jaroslav Hora, CSc.**
Katedra matematiky, fyziky a technické výchovy

Datum zadání diplomové práce: **5. února 2016**
Termín odevzdání diplomové práce: **30. června 2017**

RNDr. Miroslav Randa, Ph.D.
děkan

L.S.

Doc. PaedDr. Jarmila Honzíková, Ph.D.
vedoucí katedry

V Plzni dne 8. února 2016

OBSAH

ÚVOD

V této diplomové práci se budeme zabývat užití polynomů nad konečnými tělesy. Nejprve si definujeme konečná tělesa a vysvětlíme charakteristiku těles. Další důležitou částí této práce jsou polynomy nad konečnými tělesy. Ukážeme si operace s polynomy v $\mathbb{Z}[x]$ a také i na množině.

Vysvětlíme si ireducibilitu polynomů, neboli nerozložitelnost polynomů s celočíselnými koeficienty. Faktorizace polynomů, nebo chceme-li také řešení polynomiálních rovnic, je jedním z nejstarších problémů, kterými se matematika, respektive algebra, zabývá. Původně šlo vlastně o hledání kořenů či kořenových činitelů. V této práci si vysvětlíme pojmy ireducibilní a reducibilní mnohočlen a vysvětlíme některé algoritmy, které se dají použít k zjištění daných vlastností. Pro zjištění o nerozložitelnosti polynomů si ukážeme také algoritmus, který lze použít v $Z_p[x]$.

Další kapitolách si vysvětlíme minimální a primitivní polynomy nad konečnými tělesy, které budeme uplatňovat pro lineární kódování. Ukážeme si, na několika příkladech, jak využít metodu jejich dekódování.

V poslední kapitole se zmíníme se o některých samoopravných kódech a zároveň, kde je jejích užití.

1. KONEČNÁ TĚLESA

V této kapitole budeme pod pojmem těleso mít na mysli vždy konečné komutativní těleso, tedy množinu s dvěma binárními operacemi $(T, +, \cdot)$, kde $(T, +)$ je komutativní grupa s neutrálním prvkem 0, $(T - \{0\}, \cdot)$ je komutativní grupa s neutrálním prvkem 1, přičemž násobení je distributivní vůči sčítání.

1.1. Charakteristika tělesa

Definice 1.1.

Tělesem T nazýváme množinu (její prvky nazýváme prvky tělesa) spolu se dvěma binárními operacemi sčítání $+$ a násobení $\cdot$, které splňují sadu následujících axiomů:

(A1) $a + (b + c) = (a + b) + c$ pro libovolné $a, b, c \in T$

(A2) $a + b = b + a$ pro libovolné $a, b \in T$

(A3) existuje $0 \in T$ tak, že pro všechna $a \in T$ platí $a + 0 = 0 + a = a$

(A4) pro všechna $a \in T$ existuje $-a \in T$ tak, že platí $a + (-a) = (-a) + a = 0$

(M1) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ pro všechna $a, b, c \in T$

(M2) $a \cdot b = b \cdot a$ pro všechna $a, b, \in T$

(M3) existuje $1 \in T$ tak, že pro všechna $a \in T$ platí $1 \cdot a = a \cdot 1 = a$

(M4) pro všechna $a \neq 0$ existuje $a^{-1} \in T$ tak, že platí $a \cdot a^{-1} = a^{-1} \cdot a = 1$

(D) $a \cdot (b + c) = a \cdot b + a \cdot c$ pro všechna $a, b, c \in T$ (distributivita)

(N) $0 \neq 1$ (netrivialita)

Je-li T konečná množina, pak T je konečné těleso. Těleso K nazýváme podtělesem tělesa T, pokud K je podmnožinou T a operace sčítání $+$ a násobení $\cdot$ se v tělesech K a T shodují.

Značíme $K \leq T$. Rovněž říkáme, že T je rozšíření tělesa E.

Definice 1.2.

Nechť $(T, +, \cdot, 0, 1)$ je konečné těleso. Nejmenší přirozené číslo $r > 0$ takové, že $\underbrace{1 + 1 + \ldots + 1}_{r-krát} = 0$, se nazývá charakteristika tělesa T. Značíme $char\ T$.

Charakteristika tělesa je vlastně řád prvku 1 v grupě $(T, +)$. Pokud žádné takové r neexistuje, pak říkáme, že F má charakteristiku 0.

Tvrzení: Charakteristika konečného tělesa je vždy prvočíslo.

Důkaz:

Kdyby $char\ T = r$ bylo složené číslo, $r = a \cdot b$ pro $1 < a \leq b < r$, pak by bylo platilo:

$$0 = \underbrace{1 + 1 + \ldots + 1}_{r-krát} = \overbrace{(\underbrace{1 + 1 + \ldots + 1}_{a-krát}) + \ldots + (\underbrace{1 + 1 + \ldots + 1}_{a-krát})}^{b-krát} =$$

$$\underbrace{(1 + 1 + \ldots + 1)}_{a-krát} \cdot$$

$$\cdot \underbrace{(1 + 1 + \ldots + 1)}_{b-krát}$$

Při úpravách používáme toho, že sčítání je asociativní, je neutrální prvek vůči násobení a násobení je distributivní vůči sčítání. Protože těleso nemá dělitele nuly, musí být buď $\underbrace{1 + 1 + \ldots + 1}_{a-krát} = 0$ nebo $\underbrace{1 + 1 + \ldots + 1}_{b-krát} = 0$, což je spor s tím, že r je nejmenší takové číslo. Tudíž r je prvočíslo.

1.2. Kongruence modulo p

Definice

Nechť $p > 1$ je přirozené číslo. Na množině všech celých čísel definujeme kongruenci modulo p předpisem $x \equiv y$, pokud p dělí rozdíl $x - y$. Píšeme $x \equiv y \pmod{p}$.

Každá z p tříd této ekvivalence je tvořena všemi čísly, které při dělení číslem p dávají tentýž zbytek. Proto se označují jako zbytkové třídy modulo p. Třídu obsahující číslo x můžeme značit $[x]_p$ nebo $Z_p[x]$ a prvek x je reprezentant této třídy.

1.3. Aritmetické operace modulo *p*

Definice

Číslo p je pevně dáno. Pro třídy $[x]$ a $[y]$, zadané pomocí svých reprezentantů, je jejich součet $\oplus$ a součin $\otimes$ definován předpisy

$[x]\oplus[y]=[x+y]$

$[x]\otimes[y]=[x\,y]$.

Poznámka:

$[x]=[x']$ a $[y]=[y']$. To znamená, že $x\equiv x'$ a $y\equiv y'$. $x\equiv x'\equiv y\equiv y'$, z toho plyne $[x+y]=[x'+y']$, takže hodnota přiřazená součtu $[x]\oplus[y]$ je na volbě nezávislá. Podobně je tomu u operace $\otimes$.

Množina Z_5 má 5 prvků, které lze psát například jako $[0]_5, [1]_5, [2]_5, [3]_5, [4]_5$. Při počítání modulo p můžeme pracovat pouze s čísly $0, 1, 2, \ldots, p-1$ (s tzv. úplnou soustavou zbytků modulo p), s tím, že výsledek každé operace nahradíme příslušným zbytkem.

Ukázalo se, že pokud je p prvočíslem, je algebraická struktura $(Z_p, \oplus, \otimes)$ tělesem, které má právě p prvků. Máme tedy k dispozici konečná tělesa mající prvočíselný počet prvků. Operace v nich budeme někdy pro zjednodušení zápisu značit jen $+, \bullet$. Například při počítání modulo 5 můžeme psát $3 \oplus 4 = 2$ nebo $4 \oplus 3 = 2$. Úplnou informaci o aritmetice modulo 5 dodává tabulka:

$\oplus$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\otimes$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	1	3	2	1

Ve vektorových prostorech nad konečnými tělesy lze provádět všechny obvyklé operace jako v reálných vektorových prostorech, například řešit soustavy rovnic, hodnost matice, atd. Ještě poznamenejme, že je možné zkonstruovat konečná tělesa mající právě p^n prvků, kde p je prvočíslo. Tato tělesa se často značí $\mathrm{GF}\left(p^n\right)$, Galois field, Galoisova tělesa. V této práci budeme využívat jejich speciální případ, tělesa zbytkových tříd $Z_p{}^3$.

Příklad 1.1.

Vypočtěte soustavu čtyř rovnic o pěti neznámých nad tělesem Z_3.

$$x_1 + x_2 + 2x_3 + 2x_4 = 0$$

$$x_1 + 2x_2 + x_4 + x_5 = 2$$

$$2x_1 + x_2 + x_4 + 2x_5 = 0$$

$$x_2 + x_3 + x_4 + x_5 = 1$$

Řešení:

Nejprve soustavu lineárních algebraických rovnic vyjádříme rozšířenou maticí soustavy. Pomocí řádkovými úpravami převedeme tuto matici do tvaru, ze kterého budou určené neznámé. Upravená matice pak odpovídá soustavě rovnic, která je ekvivalentní s původní soustavou rovnic.

$$\begin{pmatrix} 1 & 1 & 2 & 2 & 0 & 0 \\ 1 & 2 & 0 & 1 & 1 & 2 \\ 2 & 1 & 0 & 1 & 2 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \approx \begin{pmatrix} 1 & 1 & 2 & 2 & 0 & 0 \\ 0 & 1 & 1 & 2 & 1 & 2 \\ 0 & 2 & 2 & 0 & 2 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \approx \begin{pmatrix} 1 & 1 & 2 & 2 & 0 & 0 \\ 0 & 1 & 1 & 2 & 1 & 2 \\ 0 & 0 & 0 & 2 & 0 & 2 \\ 0 & 0 & 0 & 2 & 0 & 2 \end{pmatrix} \approx$$

$$\approx \begin{pmatrix} 1 & 1 & 2 & 2 & 0 & 0 \\ 0 & 1 & 1 & 2 & 1 & 2 \\ 0 & 0 & 0 & 2 & 0 & 2 \\ & & & & & \end{pmatrix} \approx \begin{pmatrix} 1 & 1 & 2 & 2 & 0 & 0 \\ 0 & 1 & 1 & 2 & 1 & 2 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ & & & & & \end{pmatrix}.$$

Nejprve přičteme dvojnásobek prvního řádku k druhému řádku a prvního řádku k třetímu řádku. Poté k třetímu řádku přičteme druhý řádek a ke čtvrtému řádku přičteme druhý řádek. Třetí řádek se nyní shoduje se čtvrtým, proto čtvrtý řádek můžeme vynechat. Třetí řádek lze vynásobit 2. Po těchto úpravách zjistíme, že existují řešení soustavy.

Dostáváme: $x_4 = 1$,

$x_2 + x_3 + 2x_4 + x_5 = 2 \Rightarrow x_2 = 2x_3 + 2x_5$,

$x_1 + x_2 + 2x_3 + 2x_4 = 0 \Rightarrow x_1 = 1 + 2x_3 + x_5$

Soustava má nekonečně mnoho řešení, které závisí na parametrech.

Řešení této soustavy mají tvar $\{(1 + 2x_3 + x_5, 2x_3 + 2x_5, x_3, 1, x_5) / x_3, x_5 \in Z_3\}$.

Příklad 1.2.

Vypočtěte determinant nad tělesem Z_5:

$$\begin{vmatrix} 3 & 0 & 4 & 1 & 3 \\ 1 & 3 & 4 & 0 & 3 \\ 4 & 2 & 0 & 1 & 2 \\ 1 & 0 & 2 & 2 & 3 \\ 3 & 2 & 4 & 1 & 2 \end{vmatrix}$$

Řešení:

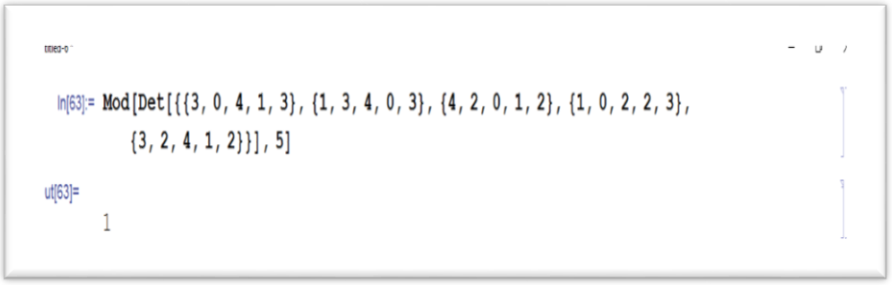
V prvním kroku provedeme prohození prvního s druhým řádkem, a zároveň nesmíme zapomenout, že pokud se mezi sebou dva řádky determinantu zamění, musíme před determinant zapsat mínus. V druhém kroku provedeme přičtení dvojnásobku prvního řádku k druhému řádku, prvního řádku k třetímu řádku, čtyřnásobku prvního řádku k čtvrtému řádku a dvojnásobku prvního řádku k pátému řádku. Ve třetím kroku přičteme trojnásobek druhého řádku ke čtvrtému řádku a dvojnásobek druhého řádku k řádku pátému. Ve čtvrtém kroku provedeme prohození třetího s pátým řádkem (determinant je

kladný). V pátém kroku přičteme ke třetímu řádku čtvrtý a pátý řádek. Posledním úkolem je vynásobit mezi sebou prvky na hlavní diagonále.

$$\begin{vmatrix} 3 & 0 & 4 & 1 & 3 \\ 1 & 3 & 4 & 0 & 3 \\ 4 & 2 & 0 & 1 & 2 \\ 1 & 0 & 2 & 2 & 3 \\ 3 & 2 & 4 & 1 & 2 \end{vmatrix} = -\begin{vmatrix} 1 & 3 & 4 & 0 & 3 \\ 3 & 0 & 4 & 1 & 3 \\ 4 & 2 & 0 & 1 & 2 \\ 1 & 0 & 2 & 2 & 3 \\ 3 & 2 & 4 & 1 & 2 \end{vmatrix} = -\begin{vmatrix} 1 & 3 & 4 & 0 & 3 \\ 0 & 1 & 2 & 1 & 4 \\ 0 & 0 & 4 & 1 & 0 \\ 0 & 2 & 3 & 2 & 0 \\ 0 & 3 & 2 & 1 & 3 \end{vmatrix} = -\begin{vmatrix} 1 & 3 & 4 & 0 & 3 \\ 0 & 1 & 2 & 1 & 4 \\ 0 & 0 & 4 & 1 & 0 \\ 0 & 0 & 4 & 0 & 2 \\ 0 & 0 & 1 & 3 & 1 \end{vmatrix} =$$

$$= \begin{vmatrix} 1 & 3 & 4 & 0 & 3 \\ 0 & 1 & 2 & 1 & 4 \\ 0 & 0 & 1 & 3 & 1 \\ 0 & 0 & 4 & 0 & 2 \\ 0 & 0 & 4 & 1 & 0 \end{vmatrix} = \begin{vmatrix} 1 & 3 & 4 & 0 & 3 \\ 0 & 1 & 2 & 1 & 4 \\ 0 & 0 & 1 & 3 & 1 \\ 0 & 0 & 0 & 3 & 3 \\ 0 & 0 & 0 & 4 & 1 \end{vmatrix} = \begin{vmatrix} 3 & 3 \\ 4 & 1 \end{vmatrix} = 3 - 2 = 1.$$

V tomto textu se také budeme snažit dokumentovat, jak je možné ověřit správnost výpočtů, kterou budeme realizovat v programu Wolfram Mathematica 8.



Příklad 1.3.

Vypočtěte hodnost matice nad tělesem Z_5:

$$A = \begin{pmatrix} 1 & 2 & 4 \\ 4 & 5 & 2 \\ 7 & 1 & 2 \end{pmatrix}, \; B = \begin{pmatrix} 1 & 2 & 3 \\ 7 & 8 & 4 \\ 4 & 5 & 1 \end{pmatrix}.$$

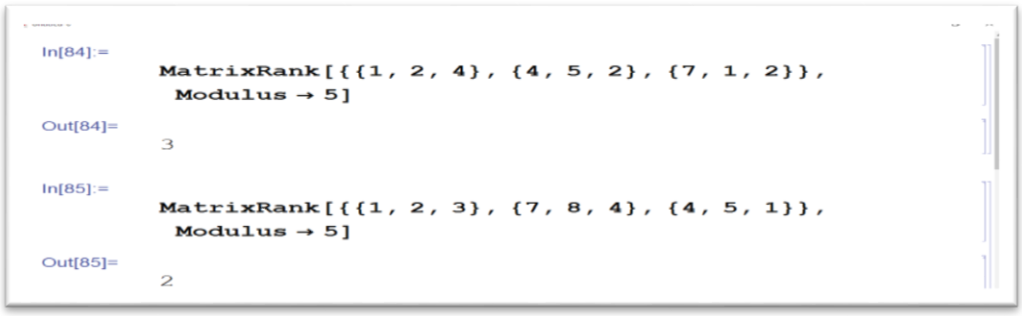
Řešení:

$$A=\begin{pmatrix}1&2&4\\4&5&2\\7&1&2\end{pmatrix}\approx\begin{pmatrix}1&2&4\\0&2&1\\0&2&4\end{pmatrix}\approx\begin{pmatrix}1&2&4\\0&2&1\\0&0&3\end{pmatrix}\Rightarrow hod\left(A\right)=3$$

V prvním kroku provedeme přičtení prvního řádku k druhému řádku a trojnásobku prvního řádku k třetímu řádku. V druhém kroku přičteme čtyřnásobek druhého řádku ke třetímu řádku. Počet řádků trojúhelníkové matice je 3, proto hodnost matice je rovna 3.

$$B=\begin{pmatrix}1&2&3\\7&8&4\\4&5&1\end{pmatrix}\approx\begin{pmatrix}1&2&3\\0&4&3\\0&2&4\end{pmatrix}\approx\begin{pmatrix}1&2&3\\0&4&3\\0&0&0\end{pmatrix}\approx\begin{pmatrix}1&2&3\\0&4&3\end{pmatrix}\Rightarrow hod\left(B\right)=2$$

V prvním kroku provedeme přičtení trojnásobku prvního řádku k druhému řádku a prvního řádku k třetímu řádku. V druhém kroku přičteme dvojnásobek druhého řádku ke třetímu řádku. Vidíme, že třetí řádek je nulový, proto ho můžeme vynechat. Počet řádků trojúhelníkové matice je 2, proto hodnost matice je rovna 2.
Nyní ověříme správnost hodností obou matic v programu.



2. POLYNOMY NAD KONEČNÝMI TĚLESY

Definice

Budiž $(T, +, \cdot)$ některé z číselných komutativních těles a n přirozené číslo. Funkci $f\left(x\right)$ definovanou předpisem $a_n x^n + a_{n-1}x^{n-1} + ... + a_2 x^2 + a_1 x^1 + a_0$, kde $a_n \neq 0$, nazýváme polynomem $n-tého$ stupně o jedné proměnné x nad tělesem $\left(T, +, \cdot\right)$.

Prvky a_n, $a_{n-1},\ldots,$ a_2, a_1, a_0 z komutativního tělesa $(T, +, \cdot)$ nazýváme koeficienty polynomu.

Pod polynomem $0-$*tého* stupně rozumíme polynom $f(x)=a_0$, kde $a_0 \neq 0$. Nulový polynom $f(x)=0$, který budeme značit $o(x)$, nemá stupeň. Polynomy, jinak také mnohočleny v $\mathbb{Z}[x]$ jsou matematické výrazy ve tvaru $a_n x^n + a_{n-1}x^{n-1} + \ldots + a_2 x^2 + a_1 x^1 + a_0 = \sum_{i=0}^{n} a_i x^i$, kde a_n, $a_{n-1},\ldots,$ a_1, a_0 jsou koeficienty polynomu, a platí a_n, $a_{n-1},\ldots,$ a_1, $a_0 \in \mathbb{Z}$ a $a_n \neq 0$, kde n – nejvyšší exponent proměnné x s nenulovým koeficientem značí stupeň polynomu.

Příkladem může být polynom $f(x)=x^4+x^2+3x+1$, kde můžeme určit jeho stupeň, který je $st(f)=4$. Mezi polynomy také patří i konstanty, v tomto případě se jedná totiž o polynomy nultého stupně (nejvyšší exponent x s nenulovým koeficientem je absolutní člen zapsaný jako $a_0 = a_0 \cdot x^0$).

Je-li polynom $p(x)=0$, pak budeme mluvit o tzv. nulovém polynomu a jeho stupeň bývá někdy definován jako $st(0)=-1$.

Definice

Nenulový polynom (zapsaný v obecném tvaru) $f(x) = a_n x^n + a_{n-1}x^{n-1} + \\ + \ldots + a_2 x^2 + a_1 x^1 + a_0$, kde koeficienty polynomu a_n, $a_{n-1},\ldots,$ a_1, $a_0 \in \mathbb{Z}$ se nazývá primitivní polynom, právě když jeho koeficienty jsou nesoudělné, tj. když největší společný dělitel $D(a_0, a_1, \ldots, a_{n-1}, a_n) = 1$.

Pro pochopení si uvedeme některé příklady primitivních polynomů např. $3x^3 - 4x^2 + 6x - 12$, $x^3 + x^2 - 1$. Je zřejmé, že z primitivního polynomu můžeme nejvýše vytknout konstantu ± 1.

2.1. Operace s polynomy

Jsou dány polynomy $f(x)=\sum_{i=0}^{n} a_i x^i$, $g(x)=\sum_{i=0}^{m} b_i x^i$, kde a_n , $b_m \neq 0$:

a) Součtem polynomů $f(x)$ a $g(x)$ je polynom $r(x)=f(x)+g(x)=\sum_{i=0}^{l}(a_i+b_i)x^i$, $l=\max(m,\ n)$, vzniklý sečtením koeficientů u proměnných se stejnými stupni.

Příklad 2.1

Sečtěte polynomy $f(x)=5x^4+2x^3+3x^2+4$ a $g(x)=x^2-x$.

Řešení:

$$f(x)+g(x)=(5x^4+2x^3+3x^2+4)+(x^2-x)=5x^4+2x^3+4x^2-x+4.$$

b) Rozdílem polynomů $f(x)$ a $g(x)$ rozumíme polynom $s(x)=f(x)-g(x)=$ $=\sum_{i=0}^{l}(a_i+b_i)x^i$, $l=\max(m,\ n)$, který vznikne odečtením koeficientů se stejnými indexy.

c) Součinem polynomů $f(x)$ a $g(x)$ je polynom $t(x)=f(x)\cdot g(x)=\sum_{i=0}^{m+n}\left(\sum_{j=0}^{i} a_j \cdot b_{i-j}\right)\cdot x^i$, který vznikne vzájemným vynásobením jednotlivých členů obou polynomů mezi sebou, a jeho výsledný stupeň je $\mathrm{st}(s)=\mathrm{st}(f)+\mathrm{st}(g)=n+m$.

Příklad 2.2

Vypočtěte součin $f(x)\cdot g(x)$, kde $f(x)=5x^4+2x^3+3x^2+4$ a $g(x)=x^2-x$.

Řešení:

$$f(x)\cdot g(x)=(5x^4+2x^3+3x^2+4)\cdot(x^2-x)=5x^6+2x^5+3x^4+4x^2-5x^5-2x^4-3x^3-4x=$$
$$=5x^6-3x^5+x^4-3x^3+4x^2-4x.$$

Další základní operací je dělení polynomu polynomem, které nelze definovat jako předešlé operace, proto se budeme podrobněji touto tématikou více zabývat.

Dělitelnost polynomů

Obecně nelze definovat podíl polynomů. Naším problémem je však zkoumat rozklad polynomů, a proto si připomeneme, jak lze realizovat dělení polynomu polynomem v případě, že koeficienty obou polynomů, leží jistém tělesu *T*. Potom bez újmy na obecnosti, můžeme předpokládat stupně polynomů $\mathrm{st}(f)=n\geq \mathrm{st}(g)=m$. Pak existují polynomy $Q(x)$ a $R(x)$, pro které platí $f(x)=Q(x)\cdot g(x)+R(x)$, kde stupeň $st(R)<st(g)$. Pokud je $R(x)=0$, platí rovnost $f(x)=Q(x)\cdot g(x)$, pak říkáme, že mnohočlen $f(x)$ je dělitelný mnohočlenem $g(x)$. Při počítání v $\mathbb{Z}[x]$ však musíme navíc sledovat, zda polynomy $Q(x)$ a $R(x)$ mají celočíselné koeficienty. Pokud by nalezené polynomy neměly celočíselné koeficienty, pak polynomy $Q(x)$ a $R(x)$ nenáleží do oboru $\mathbb{Z}[x]$.

Věta 1.1.

Budiž dány polynomy $f(x)\neq 0$, $g(x)$ z oboru integrity $(T[x],+,\cdot)$, kde $st[g(x)]\geq 1$. Potom existují polynomy $Q(x)$, $R(x)$ takové, že platí $f(x)=Q(x)\cdot g(x)+R(x)$, kde $R(x)=0$ nebo $st[R(x)]<st[g(x)]$. Tyto polynomy jsou jednoznačně určené.

Příklad 2.3

Jsou dány polynomy $f(x)=2x^4-3x^3+4x^2+5x+5$ a $g(x)=x^2-3x+2$. Nalezněte polynomy $Q(x)$ a $R(x)$ takové, že platí $f(x)=Q(x)\cdot g(x)+R(x)$.

Řešení: V tomto případě je zřejmé, že budeme dělit polynom $f(x)$ polynomem $g(x)$. Člen s nejvyšší mocninou polynomu $f(x)$ dělíme členem s nejvyšší mocninou

polynomu $g(x)$: $\frac{2x^4}{x^2} = 2x^2$, první člen $Q(x)$ je tedy $2x^2$. Tímto členem násobíme polynom $g(x)$ a výsledek odečteme od $f(x)$, dostaneme $f_1(x) = f(x) - 2x^2 \cdot g(x) = 3x^3 + 5x + 5$. Mnohočlen $f_1(x)$ nemá stupeň menší než $g(x)$, takže musíme pokračovat v dělení. Dělíme opět člen s nejvyšší mocninou $f_1(x)$ členem s nejvyšší mocninou $g(x)$: $\frac{3x^3}{x^2} = 3x$, dostáváme druhý člen polynomu $Q(x)$, kterým znovu násobíme $g(x)$ a výsledek odečteme od $f_1(x)$.

Získáváme polynom $f_2(x) = f_1(x) - 3x \cdot g(x)$. Tento polynom $f_2(x)$ má stejný stupeň jako $g(x)$, tím musíme ještě dělení jednou opakovat. Opět dělíme člen s nejvyšší mocninou $f_2(x)$ členem s nejvyšší mocninou $g(x)$: $\frac{9x^2}{x^2} = 9$, dostáváme třetí člen polynomu $Q(x)$, kterým znovu vynásobíme $g(x)$ a výsledek odečteme od $f_2(x)$.

Polynom $f_3(x) = f_2(x) - 9 \cdot g(x) = 23x - 13$. Tento polynom má již menší stupeň, než $g(x)$ a tím dělení můžeme ukončit a $f_3(x) = R(x)$ je zbytek po dělení. Jelikož polynom $Q(x) \neq 0$, není polynom $f(x)$ dělitelný $g(x)$.

Tento postup předvedeme na schématu, který jsme používali na středních školách.

$$\begin{array}{l}
\left(2x^4 - 3x^3 + 4x^2 + 5x + 5\right) : \left(x^2 - 3x + 2\right) = 2x^2 + 3x + 9 \\
-\left(2x^4 - 6x^3 + 4x^2\right) \\
\hline
\qquad 3x^3 + 5x + 5 \\
\qquad -\left(3x^3 - 9x^2 + 6x\right) \\
\hline
\qquad\qquad 9x^2 - x + 5 \\
\qquad\qquad -\left(9x^2 - 27x + 5\right) \\
\hline
\qquad\qquad\qquad 26x - 13
\end{array}$$

Zde je $Q(x)=2x^2+3x+9$ a zbytek $R(x)=26x-13$.

Tedy platí $2x^4-3x^3+4x^2+5x+5=(x^2-3x+2)\cdot(2x^2+3x+9)\ +\ (26x-13)$.

Příklad 2.4

Určete polynomy $Q(x), R(x)$ z oboru integrity polynomů $(\mathbb{Z}[x];\ +,\ \cdot)$, je – li dáno

$$f(x)=x^5-2x^4-4x^3+5x^2-5x+25,\ g(x)=x^3-2x^2+x-5.$$

Řešení:

Toto řešení je stejné jako v předchozím příkladu.

Postup je následující: $\frac{x^5}{x^3}=x^2$, takže první člen $Q(x)$ je x^2. Zpětným vynásobením a odečtením dostaneme polynom $f_1(x)=f(x)-x^2\cdot g(x)=-5x^3+10x^2-5x\ +\ 25$. Dělíme opět člen s nejvyšší mocninou $f_1(x)$ členem s nejvyšší mocninou $g(x)$: $\frac{5x^3}{x^3}=5$, což je druhý člen mnohočlenu $Q(x)$. V tomto případě je ovšem $f_2(x)=f_1(x)-5\cdot g(x)=0$ a tím můžeme ukončit dělení, protože $st(f_2)<st(g)$. Zároveň platí $f_2(x)=Q(x)$, zbytek po dělení mnohočlenu mnohočlenem je nulový, takže $f(x)$ je dělitelný $g(x)$.

Schéma: $(x^5-2x^4-4x^3+5x^2-5x+25):(x^3-2x^2+x-5)=x^2-5$

$-(x^5-2x^4+x^3-5x^2)$

$-(-5x^3+10x^2-5x+25)$

$5x^3-10x^2+5x-25$

0

Můžeme tedy konstatovat, že $f(x)$ je rozložitelný a platí $f(x)=(x^2-5)\cdot g(x)$.

Zde je $Q(x)=x^2-5$ a $R(x)=0$.

Platí tedy $x^5 - 2x^4 - 4x^3 + 5x^2 - 5x + 25 = (x^3 - 2x^2 + x - 5) \cdot (x^2 - 5)$.

2.2. Operace polynomů na množině

Následující operace sčítání a násobení si ukážeme na množině $\{0,1\}$ známe ze Z_2. V průběhu výpočtů se ukáže, že počítání s těmito polynomy je vlastně snazší než obvyklé školní operace s polynomy, které jsme si připomněli.

Vlastnosti:

na množině $\{0,1\}$ zavedeme operaci sčítání:

$$(i)\ 0 + 0 = 1 + 1 = 0$$
$$(ii)\ 1 + 0 = 0 + 1 = 1$$

na množině $\{0,1\}$ zavedeme operaci násobení:

$$(i)\ 0 \otimes 0 = 0 \otimes 1 = 1 \otimes 0 = 0$$
$$(ii)\ 1 \otimes 1 = 1$$

Příklad 2.5

Vypočtěte $f(x) + g(x)$, když jsou dány polynomy

$f(x) = x^8 + x^5 + x^4 + x + 1,\ g(x) = x^7 + x^4 + x^3 + x^2 + 1.$

Řešení:

Při sčítání polynomu $f(x)$ a $g(x)$ budeme psát posloupnosti jejich koeficientů. Koeficienty polynomu $f(x)$ napíšeme jako devítičlennou posloupnost čísel $0, 1$ v pořadí od absolutního členu ke koeficientu x^8. Stejným způsobem přepíšeme polynom $g(x)$ jako osmičlennou posloupnost čísel $0, 1$ v pořadí od absolutního členu ke koeficientu x^7. Polynom $g(x)$ tentokrát zarovnáme vlevo tak, aby absolutní členy obou polynomů byly pod sebou.

$$\begin{array}{rrrrrrrrrl} 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & f(x) \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & & g(x) \\ \hline 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & \Rightarrow x^8+x^7+x^5+x^3+x^2+x. \end{array}$$

Dostáváme výsledek polynomu $x^8+x^7+x^5+x^3+x^2+x$.

Příklad 2.6

Vypočtěte $f(x)\cdot g(x)$, když jsou dány polynomy $f(x)=x^5+x^4+x+1$, $g(x)=x^3+x^2+1$.

Řešení:

Při násobení polynomu $f(x)$ a $g(x)$ budeme opět psát posloupnosti jejich v pořadí od absolutního členu ke koeficientu u nejvyšší mocniny. Polynom $f(x)$ tvoří šestičlennou posloupnost a tuto posloupnost zarovnáme vlevo tak, aby absolutní členy obou polynomů byly pod sebou. Při násobení polynomu $g(x)$ (tvořený čtyřčlennou posloupností) polynomem $f(x)$ sečteme polynom $f(x), x^2 f(x)$ a $x^3 f(x)$.

$$\begin{array}{rrrrrrrrrl} 1 & 1 & 0 & 0 & 1 & 1 & & & & f(x) \\ 1 & 0 & 1 & 1 & & & & & & g(x) \\ \hline 1 & 1 & 0 & 0 & 1 & 1 & & & & f(x) \\ & & 1 & 1 & 0 & 0 & 1 & 1 & & x^2 f(x) \\ & & & 1 & 1 & 0 & 0 & 1 & 1 & x^3 f(x) \\ \hline 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & \Rightarrow x^8+x^6+x^5+x^2+x+1. \end{array}$$

Dostáváme výsledek polynomu $x^8+x^6+x^5+x^2+x+1$.

Příklad 2.7

Vypočtěte $f(x):g(x)$, když jsou dány polynomy $f(x)=x^6+x^5+x^3$, $g(x)=x^3+x^2$.

Řešení:

Koeficienty polynomu $f(x)$ napíšeme jako sedmičlennou posloupnost čísel $0,1$ v pořadí od absolutního členu ke koeficientu u x^6, obdobně přepíšeme i polynom $g(x)$, který je čtyřčlennou posloupností čísel $0,1$ v pořadí od absolutního členu ke koeficientu u x^3. Při dělení polynomu $f(x)$ polynomem $g(x)$ musíme nejprve polynom $x^3 g(x)$ přičíst k polynomu $f(x)$, k vzniklému polynomu přičteme $g(x)$.

$0\ 0\ 0\ 1\ 0\ 1\ 1$	$f(x)$
$0\ 0\ 1\ 1$	$x^3 g(x)$
$0\ 0\ 0\ 1\ 0\ 0\ 0$	$f(x)+x^3 g(x)$
$0\ 0\ 1\ 1$	$g(x)$
$0\ 0\ 1\ 0 \Rightarrow R(x)=x^2$	

Tím dostaneme výsledek polynomu x^3+1 a zbytek $R(x)=x^2$.

Příklad 2.8

Vypočtěte $f(x):g(x)$, když jsou dány polynomy $f(x)=x^4+x^3+x+1$, $g(x)=x^2+1$.

Řešení:

Místo samotných polynomu $f(x)$ a $g(x)$ budeme opět psát pouze posloupnosti jejich koeficientu v pořadí od absolutního členu ke koeficientu u nejvyšší mocniny. Polynom $g(x)$ zarovnáme vpravo tak, aby nejvyšší mocniny obou polynomu byly pod sebou. Při dělení polynomu $f(x)$ polynomem $g(x)$ nejprve polynom $x^2 g(x)$ přičteme k polynomu $f(x)$. K vzniklému polynomu přičteme $xg(x)$. Dalším krokem je přičtení $g(x)$. Vpravo od výpočtu jsou zapsány do schématu, jimiž jsme násobili polynom $g(x)$.

$1\ \ 1\ \ 0\ \ 1\ \ 1$	$f(x)$
$\quad\ \ 1\ \ 0\ \ 1$	$x^2 g(x)$
$1\ \ 1\ \ 1\ \ 1$	$f(x)+x^2 g(x)$
$\quad 1\ \ 0\ \ 1$	$xg(x)$
$1\ \ 0\ \ 1$	$f(x)+x^2 g(x)+xg(x)$
$1\ \ 0\ \ 1$	$g(x)$
$0 \quad \Rightarrow R(x)=0$	

Tím dostaneme výsledek polynomu x^2+x+1 a zbytek $R(x)=0$.

3.1. Ireducibilita polynomů v $\mathbb{Z}$ *x*

Eisensteinovo kritérium ireducibility

Ve školské matematice se nejčastěji zabýváme rozkladem na součin jistých polynomů s celočíselnými koeficienty, např. $x^2-9=(x-3)\cdot(x+3)$, $x^4-16=(x^2+4)\cdot(x-2)\cdot$ $\cdot(x+2)$, $x^3+64=(x+4)\cdot(x^2-4x+16)$. Polynomy $x+4$, $x^2-4x+16$ již nelze rozložit v součin polynomů prvního stupně s celočíselnými koeficienty, jak se snadno zjistí. Ovšem pro některé polynomy lze obtížně určit, zda jsou ireducibilní neboli nerozložitelné, např. pro polynom $x^7+4x^3+12x^2+8x-2$.

Definice

Buď $f(x)\in\mathbb{Z}[x]$, $f(x)\neq 0$, $f(x)\neq\pm 1$ polynom, který nelze zapsat ani jako součin dvou polynomů kladných stupňů s celočíselnými koeficienty, ani ve tvaru $f(x)=k\cdot g(x)$, $k>1$, $k\in\mathbb{Z}$, $g(x)\in\mathbb{Z}[x]$.

Tak zvaně, že z polynomu $f(x)$ není ani možné vytknout konstantu $k>1$. Pak říkáme, že polynom $f(x)$ je nerozložitelný čili ireducibilní.

Ireducibilní polynom je takový polynom, který nelze rozložit na součin jednodušších polynomů. Ireducibilními polynomy $\mathbb{Z}[x]$ jsou např. $x+1,\ x^2+x+1$. V opačném případě mluvíme o reducibilním polynomu.

Ireducibilní prvek v $\mathbb{Z}[x]$ má pouze nevlastní dělitele (jednotky a prvky s ním asociované). Ireducibilními polynomy jsou např. $x+1,\ x^2+1,\ x^4+1,$ atd.

Věta:

Mnohočlen $n-$tého stupně $f(x)=a_n\cdot x^n+a_{n-1}\cdot x^{n-1}+\ldots+a_1\cdot x+a_0$, $f(x)\in\mathbb{Z}[x]$, nelze rozložit na součin polynomů kladných stupňů s celočíselnými koeficienty, pokud existuje takové prvočíslo p, pro které platí:

i) p nedělí a_n,

ii) p dělí všechny koeficienty a_i, $i=0,\ 1,\ 2,\ \ldots,\ n-1$,

iii) p^2 nedělí a_0.

Pokud polynom vyhovuje Eisensteinovu kritériu, lze z mnohočlenu vytknout maximálně celočíselnou konstantu neboli polynom nultého stupně. Zaměříme-li se právě na vytýkání konstant, uvědomíme si, že v oboru $\mathbb{Z}[x]$ existují právě dvě čísla, která můžeme vytknout z jakéhokoliv polynomu, sice 1 a -1 (vytknutím 1 se polynom nezmění, vytknutím -1 se u všech koeficientů polynomu změní znaménka na opačná).

Jednu z podmnožin těchto polynomů dále tvoří mnohočleny, z nichž lze vytknout celé číslo různé od ±1. Například $f(x)=3x^2-27x+9=3(x^2-9x+3)$. Zjištění požadovaného koeficientu, který lze vytknout, je oproti samotnému rozkladu na součin polynomů kladných stupňů poměrně jednoduchý úkol. Jedná se vlastně jen o zjištění největšího společného dělitele koeficientů polynomu $a_n,\ a_{n-1},\ \ldots,\ a_1,\ a_0$ tj. vytknutí čísla $D(a_n,\ a_{n-1},\ \ldots,\ a_1,\ a_0)$.

Příklady 3.1.

a) Polynom $f_1=x^7+3x^4-6x^2+15$ je primitivní a splňuje podmínky Eisensteinova kritéria pro $p=3$, takže je ireducibilní v $\mathbb{Z}[x]$.

b) Polynom $f_2(x) = 5x^6 + 14x^5 - 8x^4 - 2x^3 + 4x^2 - 2$ je také ireducibilní v $\mathbb{Z}[x]$, splňuje rovněž Eisensteinovo kritérium, lze volit $p = 2$.

c) Každý polynom ve tvaru $x^n \pm p$, kde $n \in N$ a p je prvočíslo, je ireducibilní v $\mathbb{Z}[x]$.

d) Polynom $f_3(x) = x^4 + 25$ je také ireducibilní v $\mathbb{Z}[x]$. Úvahou to ověříme. Tento polynom nemá reálné kořeny a tím ani kořeny celočíselné, proto se v rozkladu polynomu $f_3(x)$ v oboru integrity $\mathbb{Z}[x]$ nemůže vyskytnout lineární faktor.

Zbývá nám možnost rozložit tento polynom na dva kvadratické faktory, tj. $f_3(x) = (x^2 + a\,x + b)(x^2 + c\,x + d)$, kde $a, b, c, d \in \mathbb{Z}$. Roznásobením a porovnáním koeficientů x^0, x^1, x^2, x^3 dostáváme soustavu čtyř rovnic o čtyřech neznámých a, b, c, d, která však nemá celočíselné řešení. Ověření tohoto faktu lze přenechat čtenáři. Hledaný rozklad $f_3(x) = (x^2 + a\,x + b)(x^2 + c\,x + d)$, kde $a, b, c, d \in \mathbb{Z}$, tedy neexistuje.

I když na polynom $f_3(x)$ nelze rovnou použít Eisensteinovo kritérium, je zde metoda, kterou je dobré znát. Píšeme – li $x = z + 1$, dostaneme polynom $F(z) = z^4 + 4\,z^3 + 6\,z^2 + 4\,z + 26$, který je ireducibilní podle Eisensteinova kritéria, $p = 2$. Pokud by existoval rozklad $f_3(x) = g(x) \cdot h(x)$, kde $g(x)$, $h(x) \in \mathbb{Z}[x]$, $st(g(x)) > 0$, $st(h(x)) > 0$, pak by muselo platit $F(z) = f_3(z+1) = g(z+1) \cdot h(z+1)$, což je spor. Je tedy tento polynom ireducibilní.

Substituce $z = x + k$, $k \in \mathbb{Z}$ mohou rozšířit oblast použitelnosti Eisensteinova kritéria, které nám již poskytly řadu ireducibilních polynomů. Nyní se budeme zajímat o algoritmy, kterými lze získat rozklad daného polynomu $f(x) \in \mathbb{Z}[x]$ v součin ireducibilních faktorů.

Pokud budeme studovat rozložitelnost polynomů v $\mathbb{Z}[x]$, mohlo by se zdát, že je příliš omezující. Existuje však úzká souvislost mezi rozložitelností v $\mathbb{Z}[x]$ a v oboru integrity

polynomů s racionálními koeficienty $\mathbb{Z}[x]$. Jak již víme, postačí nám zkoumat faktorizaci primitivních polynomů.

Věta:

Nechť $f(x) \in \mathbb{Z}[x]$ je primitivní polynom, $st(f(x)) \geq 1$. Existují – li dva polynomy $g(x)$ a $h(x) \in \mathbb{Z}[x]$ kladných stupňů tak, že $f(x) = g(x) \cdot h(x)$, pak existují též polynomy $g_1(x)$, $h_1(x) \in \mathbb{Z}[x]$ takové, že $f(x) = g_1(x) \cdot h_1(x)$. Přitom platí $g(x) = a \cdot g_1(x)$, $h(x) = b \cdot h_1(x)$, $a, b \in Z$, $a \cdot b = \pm 1$.

Kroneckerův algoritmus

Tento algoritmus je posloupnost několika kroků:

a) Při hledání jistého polynomu $g(x)$ s celočíselnými koeficienty, stupeň je menší nebo roven číslu $s = \left[\frac{n}{2}\right]$. Zde symbol $\left[\frac{n}{2}\right]$ značí tzv. celou část čísla $\left[\frac{n}{2}\right]$, tj. největší celé číslo, které je menší nebo rovno $\frac{n}{2}$. Je-li například stupeň n mnohočlenu $f(x)$ roven devíti, pak je číslo $s = \left[\frac{9}{2}\right] = 4$. Tento horní odhad pro stupeň polynomu $g(x)$ vyplývá z vlastností spjatých se součinem dvou polynomů. Pro stupně tří polynomů $f(x)$, $g_1(x)$ a $g_2(x)$, kde $f(x) = g_1(x) \cdot g_2(x)$, platí $st(f) = st(g_1) + st(g_2)$. Bez újmy na obecnosti můžeme předpokládat, že $st(g_1) \leq st(g_2)$, v opačném případě bychom provedli přečíslování. Mezním případem je zde rovnost $st(g_1) = st(g_2)$, kdy se rovnice $st(f) = st(g_1) + st(g_2)$ dá zapsat také jako $st(f) = 2 \cdot st(g_1)$, z čehož plyne $st(g_1) = \frac{st(f)}{2}$. Proto je stupeň hledaného mnohočlenu $g(x)$, který dělí polynom $f(x)$, z intervalu $1 \leq st(g) \leq s$, $st(g) \in \mathbb{Z}$.

b) Spočítáme $s+1$ funkčních hodnot mnohočlenu $f(x)$, např. pro $x = 0, 1, 2, ..., s$. Dostaneme tak $s+1$ celočíselných hodnot $f(0), f(1), f(2), ..., f(s)$.

c) Pokud má hledaný polynom $g(x)$ dělit zadaný mnohočlen $f(x)$, musí jeho funkční hodnoty v bodech $x = 0, 1, ..., s$ dělit příslušné vypočítané funkční hodnoty $f(x)$. Přesněji $g(0) \mid f(0)$, $g(1) \mid f(1)$, …, $g(s) \mid f(s)$. Zavedeme proto množiny $D_{f(0)}, D_{f(1)}, ..., D_{f(s)}$ dělitelů čísel $f(0), f(1), ..., f(s)$. To znamená, že $D_{f(0)}$ je množina všech dělitelů funkční hodnoty $f(0)$. $D_{f(1)}$ je množina všech dělitelů funkční hodnoty $f(1)$, atd., $D_{f(i)} \subset \mathbb{Z}$, $i = 0, 1, ..., s$. Zde se ukazuje, že občas je vhodnější volit body x pro výpočet funkčních hodnot $f(x)$ tak, aby tyto hodnoty měly co nejméně dělitelů. V příkladu se však budeme držet již zavedeného postupu.

Za zmínku stojí případ, kdy pro nějaké $j \in 0, 1, ..., s$ platí $f(j) = 0$. V takovém případě bychom pouhým dosazením zjistili jeden kořen polynomu $f(x)$, mnohočlen $g(x)$ by byl zapsán $g(x) = (x - j)$ a k dokončení úlohy by zbývalo dělit mnohočlen $f(x)$ nalezeným mnohočlenem $g(x)$. Získali bychom tedy rozklad $f(x) = g(x) \cdot h(x) = (x - j) \cdot h(x)$, kde $h(x) \in \mathbb{Z}[x]$ a $st(h) = st(f) - 1$. Pokud by pro žádnou funkční hodnotu $f(j)$, $j = 0, 1, ..., s$ neplatilo $f(j) = 0$, jsou všechny množiny $D_{f(0)}, D_{f(1)}, ..., D_{f(s)}$ konečné a pokračujeme dalším krokem.

d) Pomocí $s+1$ vybraných hodnot $g(0) \in D_{f(0)}$, $g(1) \in D_{f(1)}$, …, $g(s) \in D_{f(s)}$ určíme polynom $g(x)$, který v bodě $x = 0$ nabývá vybrané hodnoty $g(0)$, v bodě $x = 1$ hodnoty $g(1)$,…, v bodě $x = s$ hodnoty $g(s)$. Tento mnohočlen $g(x)$ spočteme postupem užívaným pro nalezení tzv. Newtonova interpolačního polynomu. Při hledání Newtonova interpolačního polynomu jde v podstatě o nalezení předpisu pro mnohočlen $g(x)$ kladného stupně s, přičemž známe jeho $s+1$ funkčních hodnot $f(x_i)$, kterých nabývá v $s+1$ bodech $x_i = 0$, 1, …, s. Polynom $g(x)$ zapíšeme ve tvaru

$g(x) = \lambda_0 + \lambda_1(x - x_0) + \lambda_2(x - x_0)\cdot(x - x_1) + \ldots + \quad + \lambda_s(x - x_0)\cdot\ldots\cdot(x - x_{s-1})$. Výpočet polynomu $g(x)$, respektive dopočítání koeficientů λ_0, λ_1, …, λ_s se pak dá zjednodušit zapsáním do tzv. „schématu rozdílů“:

$\Delta g(x_i) = g(x_i + 1) - g(x_i)$

$\Delta^2 g(x_i) = \Delta g(x_i + 1) - \Delta g(x_i)$

$\Delta^3 g(x_i) = \Delta^2 g(x_i + 1) - \Delta^2 g(x_i)$, atd.

$g(x_0)$			
	$\Delta g(x_0)$		
$g(x_1)$		$\Delta^2 g(x_0)$	
	$\Delta g(x_1)$		$\Delta^3 g(x_0)$
$g(x_2)$		$\Delta^2 g(x_1)$	
	$\Delta g(x_2)$		
$g(x_3)$			

Koeficienty λ_k pak spočteme dosazením do vzorce $\lambda_k = \frac{\Delta^k g(x_i)}{k!}$. Nyní si popsané kroky ukážeme na příkladu.

Příklad 3.2

Rozhodněte o ireducibilitě či reducibilitě polynomu $f(x) = x^5 + 3x^4 + 2x^3 + 2x^2 + 1$, $f(x) \in \mathbb{Z}[x]$.

Řešení: Stupeň polynomu $f(x)$ je $st(f) = 5$, hledaný mnohočlen $g(x)$ tedy bude mít stupeň nejvýše $st(g) = s = \left[\frac{5}{2}\right] = 2$. Nyní spočítáme $(s+1)$ (v tomto případě je $s+1=3$

) funkčních hodnot $f(x)$: $f(0)=1$, $f(1)=9$, $f(2)=105$ a utvoříme množiny jejich dělitelů.

$D_{f(0)}=\{1,\ -1\}$,

$D_{f(1)}=\{1,\ -1,\ 3,\ -3,\ 9,\ -9\}$,

$D_{f(2)}=\{1,\ -1,\ 3,\ -3,\ 5,\ -5,\ 7,\ -7,\ 15,\ -15,\ 21,\ -21,\ 35,\ -35,\ 105,\ -105\}$.

Množina $D_{f(0)}$ obsahuje 2 prvky, $D_{f(1)}$ jich má 6 a $D_{f(2)}$ dokonce 16. V nejhorším případě bychom tedy museli vyzkoušet všech $2\cdot 6\cdot 16=192$ uspořádaných trojic, abychom mohli konstatovat, že polynom $f(x)$ je ireducibilní.

1) Zvolíme $g(0)=g(1)=g(2)=1$. Pak ale dostáváme polynom $g(x)=1$, což je konstanta nebo též polynom nultého stupně. Konstanty ± 1 však jdou vytknout z libovolného mnohočlenu, takže budeme pokračovat v testování jiné trojice.

2) Vyzkoušíme $g(0)=1$, $g(1)=1$, $g(2)=-1$. Zde již nebude výsledkem konstanta. Vytvoříme „schéma rozdílů“.

$$\begin{array}{ccccc} 1 & & & & \\ & & 0 & & \\ 1 & & & & -2 \\ & & -2 & & \\ -1 & & & & \end{array}$$

Koeficienty λ_k pak budou: $\lambda_0=\dfrac{1}{0!}=1$,

$\lambda_1=\dfrac{0}{1!}=0$,

$\lambda_2=\dfrac{-2}{2!}=-1$.

a po dosazení do vzorce $g(x)=\lambda_0+\lambda_1(x-x_0)+\lambda_2(x-x_0)(x-x_1)$ dostaneme $g(x)=1+0\cdot(x-0)-1\cdot(x-0)(x-1)$, což po roznásobení závorek dává

$g(x) = -x^2 + x + 1$. Tento polynom $g(x)$ má sice stupeň $st(g) = 2$ a je i z oboru $\mathbb{Z}[x]$, avšak vydělíme-li jím mnohočlen $f(x)$, nedostaneme nulový zbytek. Polynom $g(x)$ tedy není dělitelem polynomu $f(x)$.

3) Nyní vyberme hodnoty $g(0) = 1,\ g(1) = 3,\ g(2) = 7$ a opět sestavíme schéma.

1			
	2		
3		2	
	4		
7			

Koeficienty λ_k jsou

$$\lambda_0 = \frac{1}{0!} = 1\ ,$$

$$\lambda_1 = \frac{2}{1!} = 2\ ,$$

$$\lambda_2 = \frac{2}{2!} = 1\ .$$

Po dosazení dostaneme $g(x) = 1 + 2 \cdot (x - 0) + 2 \cdot (x - 0)(x - 1)$ a po roznásobení máme $g(x) = x^2 + x + 1$.

Tento mnohočlen již v $\mathbb{Z}[x]$ dělí polynom $f(x)$ beze zbytku. To znamená, že jsme nalezli rozklad polynomu $f(x)$ na dva mnohočleny nižších stupňů a můžeme psát $f(x) = x^5 + 3x^4 + 2x^3 + 2x^2 + 1 = (x^2 + x + 1) \cdot (x^3 + 2x^2 - x + 1) = g(x) \cdot h(x)$, kde polynom $g(x),\ h(x) \in \mathbb{Z}$ a $st(g) \geq 1,\ st(h) \geq 1$, čímž jsme tento příklad vyřešili a zjistili, že daný polynom je reducibilní.

3. 2. Ireducibilita polynomů v $Z_p[x]$

Existuje poměrně snadný způsob jak rozhodnout, jestli je zadaný mnohočlen v daném $Z_p[x]$ rozložitelný či nikoliv. Samozřejmě je nutné si uvědomit, že v konečných tělesech může existovat jen konečné množství mnohočlenů daného stupně n.

Nabývá-li tedy stupeň polynomu a prvočíslo p nízkých hodnot, lze rozložitelnost v takovémto počtu potenciálních faktorů, který je konečný, rovnou testovat. Je-li polynom vyššího stupně nebo je-li p příliš velké, jde již zase o proces, který je vcelku výpočetně náročný.

Důležitým je následující tvrzení.

Tvrzení

Nechť $f(x)$ je polynom v $\mathbb{Z}[x]$ a $f^*(x) \in Z_p[x]$ jeho obraz v homomorfním zobrazení $j: Z[x] \to Z_p[x]$. Je-li polynom $f^*(x) \in Z_p[x]$ ireducibilní, potom je i $f(x)$ ireducibilní v $\mathbb{Z}[x]$.

Věta obrácená samozřejmě neplatí, takže je-li polynom $f^*(x) \in Z_p[x]$ rozložitelný, nevypovídá to nic o tom, že by i jeho vzor $f(x)$ v $\mathbb{Z}[x]$ byl též rozložitelný.

Berlekampův algoritmus

Rozklad mnohočlenů v $Z_p[x]$ provádíme pomocí Berlekampova algoritmu, jehož důležitou součástí je využití tzv. Petrovy-Berlekampovy matice (svůj název získala po významném českém matematiku Karlu Petrovi).

Berlekampův algoritmus se skládá ze tří kroků, a sice určení Petrovy-Berlekampovy matice, nalezení báze vlastních vektorů této matice pro vlastní hodnotu $\lambda = 1$ (dimenze báze dim(*B*) zde určuje počet faktorů) a určení netriviálního vlastního vektoru $v(x)$ a

spočtení p největších společných dělitelů $D\left(f(x), v(x)-r\right)$ pro všechny prvky $r \in Z_p$.

Nyní se podíváme podrobněji na kroky tohoto algoritmu:

1. Máme zadaný polynom $f(x) \in Z_p[x]$, jehož stupeň $st(f) = n$. Petrova-Berlekampova matice je čtvercová a počet řádků odpovídá stupni polynomu $f(x)$ (jde tedy o matici $n \times n$). Pomocí kongruence $x^{pi} \equiv q_{i,0} + q_{i,1}x + \ldots + q_{i,n-1}x^{n-1}$ modulo $f(x)$ a dopočítáme pro všechna $i = 0, 1, \ldots, n-1$ koeficienty mnohočlenů $q_{i,0} + q_{i,1}x + \ldots + q_{i,n-1}x^{n-1}$, které pak budou tvořit jednotlivé řádky Petrovy-Berlekampovy matice. Dostaneme tento tvar matice: $q_{i,0} + q_{i,1}x + \ldots + q_{i,n-1}x^{n-1}$

$$Q = \begin{pmatrix} q_{0,0} & q_{0,1} & \cdots & q_{0,n-1} \\ q_{1,0} & q_{1,1} & \cdots & q_{1,n-1} \\ \vdots & \vdots & \vdots & \vdots \\ q_{n-1,0} & q_{n-1,1} & \cdots & q_{n-1,n-1} \end{pmatrix}$$

2. Ve druhém kroku řešíme maticovou rovnost $u \cdot Q = u \cdot \lambda$, kde vlastní hodnota $\lambda = 1$ a vektor u je n-složkový. Tato rovnost vede po roznásobení na soustavu n rovnic o n neznámých. Po jejím vyřešení musíme vyjádřit bázi B vektorového podprostoru W, kam patří vektor u. Dimenze báze podprostoru W přitom určuje počet faktorů, na které lze polynom $f(x)$ rozložit.

3. V posledním kroku algoritmu vybereme jeden netriviální vektor báze B, jehož jednotlivé složky $v_0, v_1, \ldots, v_{n-1}$ poslouží jako koeficienty pro zkonstruování pomocného polynomu $v(x) = v_0 + v_1x + \ldots + v_{n-1}x^{n-1}$ a zjistíme největší společné dělitele $D\left(f(x), v(x)-r\right)$ pro všechna $r \in Z_p$ (tj. pro $r = 0, 1, \ldots, p-1$).

   Tímto postupem bychom měli obdržet faktory polynomu $f(x)$. Jejich počet pak odpovídá výše zmíněné dimenzi báze. Je-li těchto faktorů méně, než je dimenze báze, je

nutné poslední krok opakovat s jiným netriviálním vektorem báze B. Nyní si tento algoritmus ukážeme na příkladu.

Příklad 3.3

Je dán mnohočlen $f(x) = x^5 + 2x^3 + x^2 + x + 1$, $f(x) \in Z_5[x]$.

Řešení:

Určíme matici Q, kde pro $i = 0, 1, \ldots, n-1 = 0, 1, 2, 3, 4$ postupně dostaneme kongruence a z nich i řádky matice Q:

pro $i = 0$: $x^{5 \cdot 0} \equiv 1 \bmod f(x) \rightarrow$ první řádek matice Q je $(1,0,0,0,0)$,

pro $i = 1$: $x^{5 \cdot 1} \equiv 3x^3 + 4x^2 + 4x + 4 \bmod f(x) \rightarrow$ druhý řádek matice Q je $(4,4,4,3,0)$,

pro $i = 2$: $x^{5 \cdot 2} \equiv 2x^4 + 4x^3 + 4x + 2 \bmod f(x) \rightarrow$ třetí řádek matice Q je $(2,4,0,4,2)$,

Dělení polynomů budeme počítat bez formálních proměnných x:

$g(x) = x^{10}$

$f(x) = x^5 + 2x^3 + x^2 + x + 1$

0 0 0 0 0 0 0 0 0 0 1

1 1 1 2 0 1 $\qquad 4x^5 f(x)$

0 0 0 0 0 4 4 4 3 0 0

1 1 1 2 0 1 $\qquad 2x^3 f(x)$

0 0 0 2 2 1 3 4 0

1 1 1 2 0 1 $\qquad x^2 f(x)$

0 2 3 0 2 3 0

1 1 1 2 0 1 $\qquad 2 f(x)$

2 4 0 4 2 0 $\Rightarrow 2 + 4x + 4x^3 + 2x^4$.

pro $i = 3$: $x^{5 \cdot 3} \equiv 3x^3 + x^2 + 2x + 1 \bmod f(x) \rightarrow$ čtvrtý řádek matice Q je $(1,2,1,3,0)$,

$g(x) = x^{15}$

$f(x) = x^5 + 2x^3 + x^2 + x + 1$

0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1

1 1 1 2 0 1 $\quad 4x^{10} f(x)$

0 0 0 0 0 0 0 0 0 0 4 4 4 3 0 0

1 1 1 2 0 1 $\quad 2x^8 f(x)$

0 0 0 0 0 0 0 0 2 2 1 3 4 0

1 1 1 2 0 1 $\quad x^7 f(x)$

0 0 0 0 0 0 0 1 3 3 3 3 0

1 1 1 2 0 1 $\quad 2x^6 f(x)$

0 0 0 0 0 0 2 3 0 2 3 0

1 1 1 2 0 1 $\quad 2x^5 f(x)$

0 0 0 0 0 2 4 0 4 2 0

1 1 1 2 0 1 $\quad 3x^4 f(x)$

0 0 0 0 3 0 2 1 4 0

1 1 1 2 0 1 $\quad x^3 f(x)$

0 0 0 1 4 1 4 1 0

1 1 1 2 0 1 $\quad 4x^2 f(x)$

0 0 4 0 3 4 4 0

1 1 1 2 0 1 $\quad x\ f(x)$

0 1 0 1 0 4 0

1 1 1 2 0 1 $\quad f(x)$

1 2 1 3 0 0 $\Rightarrow\ 1 + 2x + x^2 + 3x^3$.

pro $i = 4 : x^{5\cdot 4} \equiv 4x^4 + 3x^3 + 2x^2 + 3x + 4 \mod f(x) \rightarrow$ poslední řádek matice Q je $(4,3,2,3,4)$.

$g(x) = x^{20}$

$f(x) = x^5 + 2x^3 + x^2 + x + 1$

0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1

1 1 1 2 0 1 $\quad 4x^{15} f(x)$

---

0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 4 4 4 3 0 0

1 1 1 2 0 1 $\quad 2x^{13} f(x)$

---

0 0 0 0 0 0 0 0 0 0 0 0 0 0 2 2 1 3 4 0

1 1 1 2 0 1 $\quad x^{12} f(x)$

---

0 0 0 0 0 0 0 0 0 0 0 0 0 1 3 3 3 3 0

1 1 1 2 0 1 $\quad 2x^{11} f(x)$

---

0 0 0 0 0 0 0 0 0 0 0 0 2 3 0 2 3 0

1 1 1 2 0 1 $\quad 2x^{10} f(x)$

---

0 0 0 0 0 0 0 0 0 0 0 2 4 0 4 2 0

1 1 1 2 0 1 $\quad 3x^9 f(x)$

---

0 0 0 0 0 0 0 0 0 0 3 0 2 1 4 0

1 1 1 2 0 1 $\quad x^8 f(x)$

---

0 0 0 0 0 0 0 0 0 1 4 1 4 1 0

1 1 1 2 0 1 $\quad 4x^7 f(x)$

---

0 0 0 0 0 0 0 0 4 0 3 4 4 0

1 1 1 2 0 1 $\quad x^6 f(x)$

---

0 0 0 0 0 0 0 1 0 1 0 4 0

1 1 1 2 0 1 $\quad x^5 f(x)$

---

0 0 0 0 0 1 2 1 3 0 0

1 1 1 2 0 1 $\quad 2x^3 f(x)$

---

0 0 0 2 2 3 1 1 0

1 1 1 2 0 1 $\quad 4x^2 f(x)$

$$\begin{array}{rrrrrrrr} 0 & 0 & 4 & 1 & 1 & 1 & 1 & 0 \\ & 1 & 1 & 1 & 2 & 0 & 1 & \\ \hline 0 & 4 & 3 & 0 & 4 & 1 & 0 & \\ 1 & 1 & 1 & 2 & 0 & 1 & & \\ \hline 4 & 3 & 2 & 3 & 4 & 0 & \Rightarrow & 4+3x+2x^2+3x^3+4x^4. \end{array} \qquad \begin{array}{l} 4x\ f(x) \\ \\ \\ 4f(x) \\ \\ \end{array}$$

Dostáváme matici v tomto tvaru:

$$Q=\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 4 & 4 & 4 & 3 & 0 \\ 2 & 4 & 0 & 4 & 2 \\ 1 & 2 & 1 & 3 & 0 \\ 4 & 3 & 2 & 3 & 4 \end{pmatrix}$$

Dále spočteme vlastní vektory, pro $\lambda=1$

dostáváme $(a,b,c,d,e)\cdot Q=(a+4b+2c+d+4e,\ 4b+4c+2d+3e,\ 4b+d+2e,$

$3b+4c+3d+3e,\ 2c+4e)=(a,b,c,d,e)$, což odpovídá soustavě rovnic:

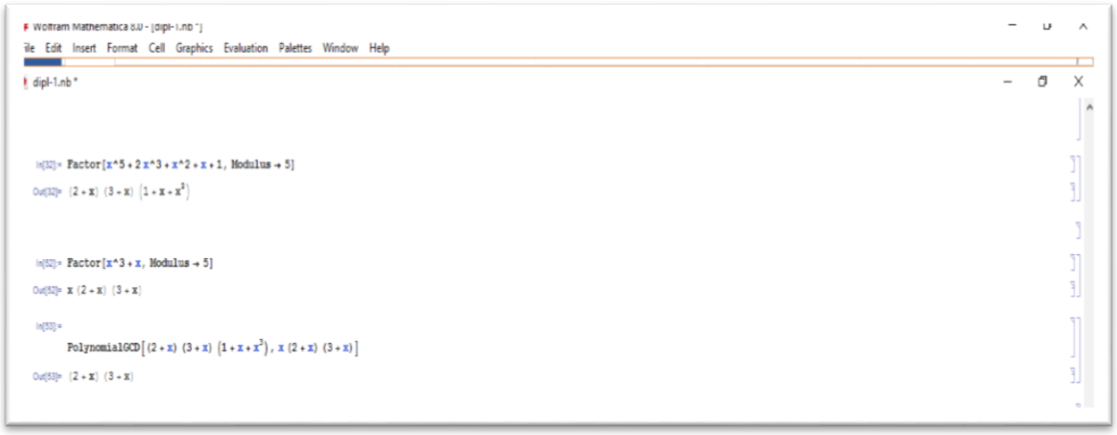
$$\begin{aligned} 4b+2c+d+4e&=0 \\ 3b+4c+2d+3e&=0 \\ 4b+d+2e&=c \\ 3b+4c+2d+3e&=0 \\ 2c+3e&=0 \end{aligned}$$

Volíme-li neznámé $b=v$ a $c=w$ jako parametry, dostaneme $d=v+4w,\ e=w$ a neznámá a je libovolná hodnota z $Z_5[x]$, tedy $a=u$. Vektorový prostor je tak možné popsat pomocí parametrů $u,v,w\in Z_5[x]$ jako $W=\{(u,v,w,v+4w,w)\}$. Jeho bází je například $B=\{(1,0,0,0,0),\ (0,1,0,1,0),\ (0,0,1,4,1)\}$. Mnohočlen $f(x)$ je možné v $Z_5[x]$ rozložit v součin tří faktorů, protože dimenze báze $\dim(B)=3$.

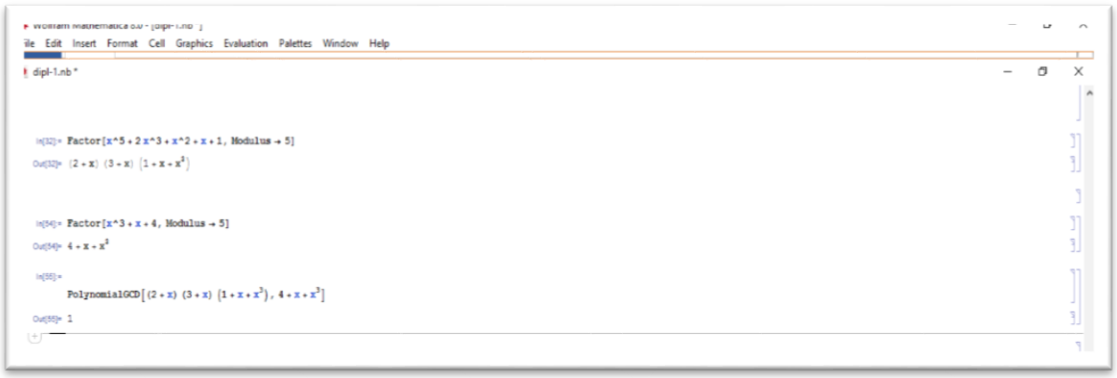
Zvolíme-li pro další postup vektor $(0,1,0,1,0)$, dostáváme pomocný mnohočlen $v(x) =$ $= x^3 + x$ a podle postupu určíme pět $(pro\ r = 0, 1, \ldots, 4)$ největších společných dělitelů $D(f(x), v(x) - r)$:

Pro určování největších společných dělitelů dvou polynomů využijeme programu Wolfram Mathematica 8.

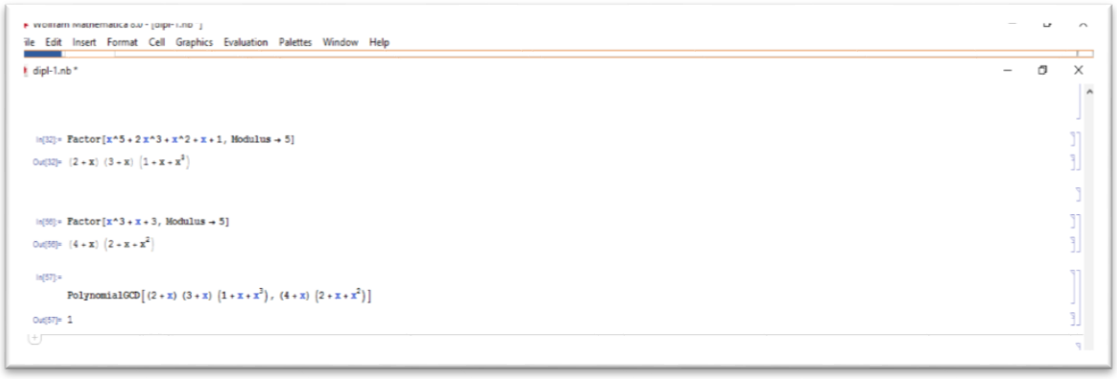
$r = 0: D(f(x), v(x) - 0) = D(x^5 + 2x^3 + x^2 + x + 1, x^3 + x) = (3 + x)(2 + x),$



$r = 1: D(f(x), v(x) - 1) = D(x^5 + 2x^3 + x^2 + x + 1, x^3 + x + 4) = 1,$

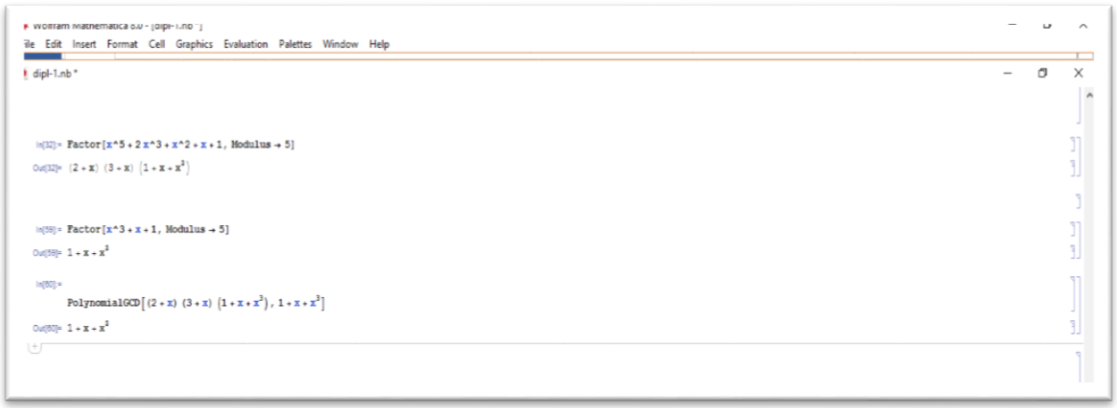


$r = 2: D(f(x), v(x) - 2) = D(x^5 + 2x^3 + x^2 + x + 1, x^3 + x + 3) = 1,$



$$r=3: D\left(f(x), v(x)-3\right) = D\left(x^5+2x^3+x^2+x+1, x^3+x+2\right)=1,$$

$$r=4: D\left(f(x), v(x)-4\right) = D\left(x^5+2x^3+x^2+x+1, x^3+x+1\right) = x^3+x+1.$$



Zjišťujeme tři ireducibilní faktory polynomu $f(x)$, které při vzájemném násobení v $Z_5[x]$ dávají výsledek $(x^3+x+1)(x+3)(x+2) = x^5+2x^3+x^2+x+1.$ Nalezli

jsme tedy rozklad polynomu $f(x)$ v $Z_5[x]$, který zapíšeme $f(x)=(x^3+x+1)(x+3)(x+2)$.

4. MINIMÁLNÍ A PRIMITIVNÍ POLYNOMY

Nyní se zaměříme na hledání minimálních polynomů prvků tělesa. Buď θ takový prvek tělesa F_{q^m}, že $\{1, \theta, \ldots, \theta^{m-1}\}$ tvoří bázi F_{q^m} nad F_q. Pokud chceme najít minimální polynom f prvku $\beta \in F_{q^m}$ nad F_q, vyjádříme mocniny $1, \beta, \beta^2 \ldots, \beta^{m-1}$ pomocí této báze.

Tedy

$$\beta^i = \sum_{j=0}^{m} b_{ij}\, \theta^j \qquad pro \;\; 0 \le i \le m.$$

Nechť $f(x) = a_m x^m + a_{m-1}x^{m-1} + \ldots + a_1 x + a_0$. Pak z podmínky $f(\beta) = 0$ dostáváme

$$\sum_{i=0}^{m} a_i b_{ij} = 0 \qquad pro \;\; 0 \le j \le m-1.$$

Máme tedy homogenní soustavu m lineárních rovnic o $m+1$ neznámých. Rovnice zapíšeme do matice $A=(a_{ij})$ typu $m \times (m+1)$ takové, že $(a_{ij}) = b_{j+1,\,i+1}$. Tudíž se jedná o matici, jejíž $i-$tý sloupec je tvořen zápisem β^{i-1} v dané bázi. Takže je zřejmé, že jde o matici naší soustavy. Označíme h hodnost matice A. Pak prostor řešení dané soustavy má dimenzi $d = m+1-h$. Protože $1 \le h \le m$, platí $1 \le d \le m$. Nyní lze položit $a_m = a_{m-1} = \cdots = a_{m-d+2} = 0$ a $a_{m-d+1} = 1$. Ostatní koeficienty polynomu dopočítáme ze soustavy. Nyní předvedeme tuto metodu na následujícím příkladu.

Příklad 4.1

Je dán $\theta \in F_{64}$ kořen ireducibilního polynomu $f(x) = x^6 + x + 1$ v $F_2[x]$. Nalezněte minimální polynom prvku $\beta = 1 + \theta^2 + \theta^3$ nad F_2.

Řešení:

Napíšeme si nejprve mocniny β vyjádřené v bázi $1, \theta^2, \theta^3, \ldots, \theta^5$. Máme

$\beta^0 = 1$

$\beta^1 = 1 \quad + \theta^2 + \theta^3$

$\beta^2 = \quad \theta \quad + \theta^4$

$\beta^3 = 1 + \theta + \theta^2 + \theta^3$

$\beta^4 = \quad \theta^3$

$\beta^5 = 1 + \theta \quad + \theta^3 \quad + \theta^5$

$\beta^6 = \quad \theta + \theta^2 \quad + \theta^4$

Matice A je tedy dána

$$\begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \approx \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \approx \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \approx$$

$$\approx \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

Hodnost matice je $h = 6$ a $d = 6 + 1 - 6 = 1$. Zvolme tedy $a_6 = 1$ a dopočteme ostatní koeficienty. Dostáváme $a_5 = 0$; $a_4 = 1$; $a_3 = 0$; $a_2 = 1$; $a_1 = 1$; $a_0 = 1$. Z těchto koeficientů jsme získali minimální polynom nad F_2. Tento minimální polynom je tedy $x^6 + x^4 + x^2 + x + 1$.

Ukážeme si další metodu na hledání minimálních polynomů, která je založena na následující větě.

Věta:

Buď $\alpha \in F_{q^m}$. Nechť g je minimální polynom prvku α nad F_q, který má stupeň d. Pak kořeny g jsou prvky $\alpha, \alpha^q, \ldots, \alpha^{q^{d-1}}$ a je g minimální polynom všech těchto prvků nad F_q.

Z této uvedené věty vyplývá, pro nalezení minimálního polynomu f prvku F_{q^m} nad F_q stačí spočítat mocniny $\beta, \beta^q, \ldots, \beta^{q^{d-1}}$, kde d je nejmenší přirozené číslo takové, že $\beta^{q^d} = \beta$. Potom $f(x) = (x-\beta)(x-\beta^q)\cdots(x-\beta^{q^{d-1}})$.

Druhým způsobem je nalezení primitivního prvku vhodného tělesa a konstrukce jeho minimálního polynomu. Přesněji, pokud chceme sestrojit primitivní polynom stupně m nad F_q, najdeme primitivní prvek tělesa F_{q^m} a sestrojíme jeho minimální polynom některou z uvedených metod. Prvek F_{q^m} je primitivní, právě když má v grupě $F^*_{q^m}$ řád $q^m - 1$. Nechť je $q^m - 1 = k_1 \cdots k_l$ rozklad na součin po dvou nesoudělných přirozených čísel. Pro každé $1 \le i \le l$ nalezneme prvek $\alpha_i \in F^*_{q^m}$ řádu k_i. Poté $\alpha = \alpha_1 \alpha_2 \cdots \alpha_l$ má řád $q^m - 1$. Tudíž je α primitivní prvek a sestrojením jeho minimálního polynomu dostaneme požadovaný primitivní polynom.

Definice

Buď f nenulový polynom nad F_q. Pokud $f(0) \neq 0$, definujeme řád polynomu f jako nejmenší k přirozené číslo, že $f(x)$ dělí $x^k - 1$. V opačném případě platí $f(x) = x^l g(x)$, kde $l \in N$, $g \in F_q[x]$. Pak řád polynomu f definujeme jako řád g. Řád f značíme $ord(f)$.

Předchozí definice je korektní, protože pro každý polynom $f \in F_q[x]$, $g(0) \neq 0$ stupni $m \ge 1$ platí, že existuje přirozené číslo $k \le q^m - 1$,pro něž $f(x)$ dělí $x^k - 1$,

Nyní si uvedeme základní vlastnosti řádu polynomu a také si ukážeme, jak je možné řád polynomu spočítat. Nejprve je dobré si uvědomit elementární vlastnost řádu polynomu, která připomíná řád prvku.

Pro přirozené číslo k a polynom $f \in F_q[x]$, $f(0) \neq 0$ platí: f dělí $x^k - 1$, právě když $ord(f)$ dělí k. Dále si všimneme, jaký význam má řád pro ireducibilní polynomy.

Tvrzení: Řád ireducibilního polynomu f stupně m nad tělesem F_q, který splňuje $f(0) \neq 0$, je roven řádu jeho libovolného kořene v grupě $F_{q^m}^*$. Důsledkem je řád ireducibilního polynomu f stupně m nad tělesem F_q, který dělí $q^m - 1$. Pro reducibilní polynomy toto tvrzení ani jeho důsledek nemusí platit, ale řád reducibilního polynomu dokážeme spočítat z řádů jeho ireducibilních faktorů. To nám ukáží následující tvrzení.

Tvrzení: Pokud $f \in F_q[x]$ je součinem po dvou nesoudělných polynomů nad F_q, pak řád f je roven nejmenšímu společnému násobku jejich řádů.

Tvrzení: Označme p charakteristiku F_q tělesa. Nechť g je ireducibilní polynom nad F_q řádu k splňující $g(0) \neq 0$ a buď $f = g^m, kde\ m \in N$. Pak $ord(f) = kp^l$, kde $l \in N \cup \{0\}$ je nejmenší takové, že $p^l \leq m$.

Z těchto dvou tvrzení bezprostředně vyplývá následující věta pro určení řádu polynomu.

Věta:

Označme p charakteristiku tělesa F_q. Buď f polynom kladného stupně nad F_q splňující $f(0) \neq 0$. Buď $f = a{g_1}^{m_1} \cdots a{g_n}^{m_n}$, $a \in F_q$, $m_1, \ldots, m_n \in N$ rozklad f na součin monických ireducibilních polynomů. Pak $ord(f) = kp^l$, kde k je rovno nejmenšímu společnému násobku čísel $ord(g_1), \ldots, ord(g_n)$ a $l \in N \cup \{0\}$ je nejmenší takové, že $p^l \geq \max\ m_1, \ldots, m_n$.

S pomocí těchto tvrzení vypočteme a dokážeme několik příkladů, které ilustrují

popsané metody, případně popisují další vlastnosti řádu. Nejprve si ukážeme použití této uvedené věty.

Příklad 4.2

Určete řád polynomu $f(x)=\left(x^2+x+1\right)^5\left(x^3+x+1\right)$ nad Z_2.

Řešení:

Označíme $g(x)=\left(x^2+x+1\right), h(x)=\left(x^3+x+1\right)$. Snadno se ověří, že g,h jsou ireducibilní polynomy nad F_2. Z toho plyne, že $ord\ g\ x$ dělí $2^2-1=4-1=3$. Je evidentní, že $ord\ g\ x\ \geq 3$, tudíž $ord\ g\ x\ =3$. Obdobně $ord\ h\ x$ dělí $2^3-1=8-1=7$ a $ord\ h\ x\ >1$, takže $ord\ h\ x\ =7$. Z věty dostáváme $ord\ f\ =kp^l$, kde $k=21; p=2; l=3$. Tedy $ord\ f\ =21\cdot 8=168$.

Dále se zaměříme na jiné možnosti jak určit řád polynomu, jedná se o speciální případy, kdy všechny kořeny polynomu jsou jednoduché nebo je polynom ireducibilní a podobně.

Definice

Buď F těleso charakteristiky p a nechť n je přirozené číslo, p nedělí n. Pak definujeme n - tý cyklotomický polynom jako $Q_n\ x\ =\prod_{\xi}\ x-\xi$, kde násobení probíhá přes všechny primitivní n-té odmocniny z jedné. Tento součin probíhá v rozkladovém nadtělese F určeném polynomem x^n-1, v němž existují primitivní n-té odmocniny z jedné.

Je zřejmé, že Q_n je možno ekvivalentně definovat jako $Q_n\ x\ =\prod_{\substack{s=1 \\ NSD=\ s,n\ =1}}^{n}\ x-\xi^s$, kde ξ je libovolná primitivní n-tá odmocnina z jedné.

Polynom stupně n z $F_q\ x$ nazveme primitivním polynomem nad F_q, pokud je minimálním polynomem nad F_q primitivního prvku tělesa F_{q^n}.

Následující věta uvádí do souvislosti pojem primitivního polynomu a řád polynomu.

Víme, že polynom nad F_q stupni n má řád menší nebo roven $q^n - 1$. Pro primitivní polynomy platí rovnost.

Polynom $f \in F_q\ x$ stupně n je primitivní nad F_q, právě když f je monický, $f(0) \neq 0$ a $ord(f) = q^n - 1$.

Na následujících příkladech si ukážeme několik základních vlastností primitivních polynomů, které lze ověřit, zda zadaný polynom je primitivní.

Mějme polynom $f(x) = x^6 + x^5 + x^2 + x + 1$, který je primitivní polynom nad tělesem F_2.

Tento zadaný polynom $f(x) = x^6 + x^5 + x^2 + x + 1$, ověříme velmi snadno. Dosadíme $f(0) = 0^6 + 0^5 + 0^2 + 0 + 1 \neq 0$, z toho vidíme, že tento polynom je monický a podle věty stačí ukázat, že $ord(f) = 2^6 - 1 = 63$. Protože ireducibilní polynomy $x+1,\ x^2 + x + 1,$ $x^3 + x + 1, x^3 + x^2 + 1$ nedělí f, je f ireducibilní. Dále $ord(f) \mid 63$ a řád polynomu je určitě větší nebo roven jeho stupni a proto pro polynomy $x^7 + 1, x^9 + 1, x^{21} + 1$ snadno ověříme, že je f nedělí. Tedy $ord(f) = 63$ a z toho plyne, že polynom $f(x) = x^6 + x^5 + x^2 + x + 1$ je primitivní.

Buď $f \in F_q\ x$ monického stupně $n \geq 1$. Dokažte, že f je primitivní nad F_q, právě když f je ireducibilní faktor nad F_q cyklotomického polynomu $Q_d \in F_q\ x$, kde $d = q^n - 1$.

Buď naopak f ireducibilní faktor Q_d. Nechť je α kořen f. Pak je α primitivní $(q^m - 1)$-*tá* odmocnina z jedné, tedy α je primitivní prvek tělesa F_{q^m}. Polynom f je monický a ireducibilní, tudíž je minimálním polynomem prvku α, a tedy se jedná o primitivní polynom.

Příklad 4.3

Určete počet primitivních polynomů stupně m nad F_q.

Řešení:

Z příkladu plyne, že stačí určit počet ireducibilních faktorů polynomu Q_d, kde $d = q^m - 1$. Označíme ho k. Protože čísla q, d jsou nesoudělná, platí $k = \varphi(d)/m = \varphi(q^m - 1)/m$.

Příklad 4.4

Je dán polynom $f(x) = x^3 + x + 1 \in Z[x]$. Platí, že množina všech polynomů s koeficienty v Z_2 stupně rovného nebo menšího než 2 s operacemi sčítání a násobení modulo $x^3 + x + 1$ je těleso. Naleznětě inverzní prvek k polynomu $p(x) = x + 1$.

Řešení:

Vezměme polynom $(x+1)$. Nejprve nalezneme polynom $(x+1)^{-1}$ inverzní k $(x+1)$. Dalším krokem využijeme rozšířeného Eukleidova algoritmu, a tím nalezneme polynomy $a(x), b(x) \in Z_2[x]$ takové, aby platilo $a(x) \cdot (x+1) + b(x) \cdot f(x) = 1$. Nalezli jsme polynomy $x^3 + x + 1 = (x+1) \cdot (x^2 + x) + 1$, z toho je patrně vidět inverzní polynom $(x+1)^{-1} = x^2 + x$. Tento postup použijeme vždy, když největší společný dělitel $f(x) \in F[x]$ a libovolný nenulový polynom z $F[x]$ stupně menšího než je stupeň $f(x)$ je roven 1.

Pro některé polynomy tento postup neplatí, například pro polynom $f(x) = x^3 + x = x \cdot (x^2 + 1)$.

Pro náš účel se jeví jako poměrně důležitá část počítačové algebry studium faktorizace polynomů nad tzv. konečnými tělesy. Polynom v oboru $Z_p[x]$, kde p je prvočíslo, zapíšeme ve tvaru $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_2 x^2 + a_1 x^1 + a_0$. Přitom koeficienty a_n, $a_{n-1}, \ldots, a_2, a_1, a_0 \in Z_p$, což znamená, že tyto koeficienty mohou nabývat jen hodnot z množiny $\{0, 1, \ldots, p\}$. Součty, rozdíly, součiny a podíly polynomů i jejich derivování

jsou prováděny podobně jako v $\mathbb{Z}[x]$, avšak s rozdílem, že koeficienty získaného výsledku opět patří do Z_p.

5. LINEÁRNÍ KÓDY

Lineární kód je v teorii kódování typem blokového kódu používaným metodami pro detekci a opravu chyb. Lineární kódy umožňují realizaci efektivnějších algoritmů pro kódování a dekódování než jiné kódy.

5.1. Elementární kódy

Ukážeme si několik příkladu elementárních kódu vycházejících z technických možností své doby.

Kódy *k* z *n*

Kódy mají *n*-místné značky. V každé značce je právě k jedniček. Kontrola přijatých značek spočívá ve spočítání jedniček v přijaté značce.

Příklad 5.2

Kód *2* z *5*

0 0 0 1 1
0 0 1 0 1
0 1 0 0 1
1 0 0 0 1
0 0 1 1 0
0 1 0 1 0
1 0 0 1 0
0 1 1 0 0
1 0 1 0 0
1 1 0 0 0

5.2. Jednoduchý paritní kód

Paritní bity se používají při komunikaci po sériové lince. Všechna data uložená v našich počítacích se skládají z nul a jedniček. Jsou to informace, které obsahují jen dvě možnosti

(jedna-nula, ano-ne, zapnuto-vypnuto). Tyto možnosti mají vždy velikost jednoho bitu. Nuly a jedničky skládáme do slov. Tato slova mohou mít různou délku. Slovo, které má délku osm bitu, nazýváme byte. Snadnou metodou pro zjištění možnosti chyby při přenosu datového slova je použití paritního bitu. Paritní bit je takový bit, který přidáme k datovému slovu. Je to poslední bit v rámci datového slova. Ten obsahuje informaci o počtu jedničkových bitu v našem slově.

Pokud je v původním slově počet jedniček sudý, přidáme nulu, v opačném případě jedničku.

Tabulka 1

1.	*a*	111011001010000	7
2.	*b*	011101100101000	7
3.	*c*	100110101111000	8
4.	*d*	001110110010100	7
5.	*e*	110101111000100	8
6.	*f*	010011010111100	8
7.	*g*	101000011101100	7
8.	*h*	000111011001010	7
9.	*i*	111100010011010	8
10.	*j*	011010111100010	8
11.	*k*	100001110110010	7
12.	*l*	001001101011110	8
13.	*m*	110010100001110	7
14.	*n*	010100001110110	7
15.	*o*	101111000100110	8
16.	*p*	000011101100101	7
17.	*q*	111000100110101	8
18.	*r*	011110001001101	8
19.	*s*	100101000011101	7
20.	*t*	001101011110001	8

21.	*u*	110110010100001	7
22.	*v*	010000111011001	7
23.	*x*	101011110001001	8
24.	*y*	000100110101111	8
25.	*z*	111111111111111	15
26.	*mezera*	011001010000111	7
27.	*tečka*	100010011010111	8
28.	*,*	001010000111011	7
29.	*:*	110001001101011	8
30.	*?*	010111100010011	8
31.	*!*	101100101000011	7
32.	*“*	000000000000000	0

V této tabulce je 32 patnáctičlenných posloupností složených z prvků $0,1$. Každá patnáctičlenná posloupnost v této tabulce je kódové slovo. Kód je množina kódových slov. V prvním sloupci tabulky je napsáno pořadí, v druhém sloupci písmena abecedy a některá interpunkční znaménka, ve třetím sloupci jsou jednotlivá kódová slova. Čísla uvedená ve čtvrtém sloupci tabulky udávají počet jedniček v jednotlivých kódových slovech, ten se nazývá váha slova.

Součet dvou kódových slov je opět kódové slovo,

např. $m+a=l$	např. $b+c=a$	např. $mez+i=s$
110010100001110	011101100101000	011001010000111
111011001010000	100110101111000	111100010011010
001001101011110	111011001010000	100101000011101

Lineární blokový kód je pravidelný *n*-místný kód, kde množina vektorů přiřazená značkám tvoří podprostor vektorového prostoru.

Kód, ve kterém je součet dvou kódových slov opět kódové slovo, se nazývá lineární (grupový). Vzdáleností dvou slov (nemusí být kódová) se rozumí váha jejich součtu.

Pravidlo pro dekódování:

Jestliže v přijatém slově jsou nejvýše tři chyby, nalezneme správné kódové slovo tak, že vezmeme kódové slovo, jehož vzdálenost od přijatého slova je nejvýš rovna třem. Příklad vzájemného přirazení vektoru a značek je znázorněn schématem:

Množina vektoru	*Kódovací tabulka*
$v_1 = (0\,0\,0\,0\,0)$	x_1 0 0 0 0 0
$v_2 = (1\,0\,0\,0\,1)$	x_2 1 0 0 0 1
$v_3 = (0\,1\,0\,1\,0)$	x_3 0 1 0 1 0
$v_4 = (0\,0\,1\,1\,1)$	x_4 0 0 1 1 1
$v_5 = (1\,1\,0\,1\,1)$	x_5 1 1 0 1 1
$v_6 = (1\,0\,1\,1\,0)$	x_6 1 0 1 1 0
$v_7 = (0\,1\,0\,1\,1)$	x_7 0 1 0 1 1
$v_8 = (1\,1\,1\,0\,0)$	x_8 1 1 1 0 0

Příklad 5.1

Byla přijata zpráva, která je tvořena řádky následující tabulky:

000011101100101

101111000100110

010111111110111

101111000100110

011110001001101

101100101000011.

Řešení:

Pokud při přenosu zprávy nevznikly žádném kódovém slově více než tři chyby, můžeme přijatou zprávu dešifrovat za pomoci tabulky 1 a pravidla dekódování. První řádek odpovídá kódovému slovu p , druhý řádek slovu o , třetímu řádku neodpovídá žádné kódové slovo z tabulky 1, čtvrtý řádek opět slovu o , pátý řádek slovu r a šestému řádku odpovídá slovo !. Dešifrovaný text je $PO\_OR!$.

Spočítáme vzdálenost nerozšifrovaného slova od kódového slova. Zjistíme, že slovo ve třetím řádku má od kódového slova vzdálenost 3, přičemž k chybám došlo na 1., 3. a 12. místě. Rozšifrovaná zpráva tudíž zní *POZOR*!.

5.3. Maticový popis lineárního kódu

Souřadnice vektoru báze prostoru V_1 zapíšeme do řádku matice. Získáme tím matici G kódu.

$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{pmatrix}$ tj. generující matice kódu.

Vektory značek kódu jsou lineární kombinací řádku matice G. Prostor vektorů V_2 je ortogonální ke všem vektorům V_1. Prostor pojmenovaný V_2 má generující matici, kterou nazveme H.

$H = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{pmatrix}$ je kontrolní matice kódu. Platí-li $v \cdot H^T = 0$, vektor v je vektorem značky kódu.

Příklad 5.2

$$v_1 \cdot H^T = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \\ 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & + & 0 & + & 0 & + & 0 & + & 0 \\ 1 & + & 0 & + & 0 & + & 0 & + & 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} = 0$$

$$v_2 \cdot H^T = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \\ 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & + & 1 & + & 0 & + & 1 & + & 0 \\ 0 & + & 0 & + & 0 & + & 0 & + & 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} = 0,$$

$$v_3 \cdot H^T = \begin{pmatrix} 0 & 1 & 1 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \\ 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & + & 1 & + & 1 & + & 0 & + & 0 \\ 0 & + & 0 & + & 1 & + & 0 & + & 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} = 0 .$$

Kód má minimální vzdálenost $d_{\min}$ rovnu w v případě, že libovolná množina $w-1$ a méně než $w-1$ řádku matice H^T je nezávislá, zatímco alespoň jedna množina w řádku je závislá.

5.4. Systematický lineární kód

Každý lineární kód je možné převést na systematický kód se stejnou zabezpečovací schopností.

Lze použít tyto elementární úpravy:

a) Vzájemná výměna řádku - kód se nemění.

b) Přičtení řádku k jinému - kód se nemění.

c) Vzájemná výměna sloupců - kód se mění na jiný kód se stejnou zabezpečovací schopností.

V oblasti kódování je pojem syndrom S velmi důležitý. Je dán vztahem $S = v \cdot H^T$. Je to vektor s $n-k$ prvky.

5.5. Algebraická metoda dekódování

Tato metoda vede k cíli celkem rychle i v případě kódu větší délky a s více kódovými slovy.

Tabulka 2

$$\alpha^4 = \alpha + 1$$

$$\alpha^5 = \alpha^2 + \alpha$$

$$\alpha^6 = \alpha^3 + \alpha^2$$

$$\alpha^7 = \alpha^4 + \alpha^3 = \alpha^3 + \alpha + 1$$

$$\alpha^8 = \alpha^5 + \alpha^4 = \alpha^2 + \alpha + \alpha + 1 = \alpha^2 + 1$$

$$\alpha^9 = \alpha^6 + \alpha^5 = \alpha^3 + \alpha^2 + \alpha^2 + \alpha = \alpha^3 + \alpha$$

$$\alpha^{10} = \alpha^7 + \alpha^6 = \alpha^3 + \alpha + 1 + \alpha^3 + \alpha^2 = \alpha^2 + \alpha + 1$$
$$\alpha^{11} = \alpha^8 + \alpha^7 = \alpha^2 + 1 + \alpha^3 + \alpha + 1 = \alpha^3 + \alpha^2 + \alpha$$
$$\alpha^{12} = \alpha^9 + \alpha^8 = \alpha^3 + \alpha + \alpha^2 + 1 = \alpha^3 + \alpha^2 + \alpha + 1$$
$$\alpha^{13} = \alpha^{10} + \alpha^9 = \alpha^2 + \alpha + 1 + \alpha^3 + \alpha = \alpha^3 + \alpha^2 + 1$$
$$\alpha^{14} = \alpha^{11} + \alpha^{10} = \alpha^3 + \alpha^2 + \alpha + \alpha^2 + \alpha + 1 = \alpha^3 + 1$$
$$\alpha^{15} = \alpha^{12} + \alpha^{11} = \alpha^3 + \alpha^2 + \alpha + 1 + \alpha^3 + \alpha^2 + \alpha = 1$$

Prvku α a jeho patnácté mocniny, lze snadno zjistit další mocniny prvku α, které jsou rovny 1. $\alpha^{15} = 1 \Rightarrow \alpha^{30} = \left(\alpha^{15}\right)^2 = \alpha^{45} = \left(\alpha^{15}\right)^3 = \ldots = 1$.

Prvních patnáct mocnin prvku α udává všechny jeho mocniny. Každou mocninu prvku α můžeme převést na polynom proměnné a stupně maximálně 3. Po sečtení několika takových polynomů dostaneme polynom nulový nebo polynom nejvýše stupně 3, který bude vždy odpovídat některé mocnině prvku α podle tabulky 2.

Například:

$\alpha^{15} + \alpha^{10} + \alpha^8 = 1 + \alpha^2 + \alpha + 1 + \alpha^2 + 1 = \alpha + 1$.

Tabulka 3

1.	1	17.	$x^4 + 1$
2.	x	18.	$x^4 + x$
3.	$x + 1$	19.	$x^4 + x + 1$
4.	x^2	20.	$x^4 + x^2$
5.	$x^2 + 1$	21.	$x^4 + x^2 + 1$
6.	$x^2 + x$	22.	$x^4 + x^2 + x$
7.	$x^2 + x + 1$	23.	$x^4 + x^2 + x + 1$
8.	x^3	24.	$x^4 + x^3$
9.	$x^3 + 1$	25.	$x^4 + x^3 + 1$
10.	$x^3 + x$	26.	$x^4 + x^3 + x$

11.	x^3+x+1	27.	x^4+x^3+x+1
12.	x^3+x^2	28.	$x^4+x^3+x^2$
13.	x^3+x^2+1	29.	$x^4+x^3+x^2+1$
14.	x^3+x^2+x	30.	$x^4+x^3+x^2+x$
15.	x^3+x^2+x+1	31.	$x^4+x^3+x^2+x+1$
16.	x^4	32.	0

Vynásobíme-li tento polynom $f(x)=1+x+x^2+x^4+x^5+x^8+x^{10}$ postupně polynomy maximálně stupně 4, nesmíme zapomenout na nulový polynom v tabulce 3. Pokud přepíšeme koeficienty vzniklých polynomů jako patnáctičlenné posloupnosti čísel $0,1$, dostáváme se k tabulce 1. To znamená, že polynom $f(x)$ generuje kód z tabulky 1.

Správně přijatá slova

Slovo délky 15 je kódové slovo v případě, že příslušný polynom je dělitelný polynomem $f(x)$. Podíl určuje kódové slovo: Je-li podíl na k -tém místě tabulky 3, je příslušné slovo k -tým kódovým slovem v tabulce 1.

Například:

Kódové slovo n v tabulce 1 vydělíme polynomem $f(x)=1+x+x^2+x^4+x^5+x^8+x^{10}$.

0	1	0	1	0	0	0	0	1	1	1	0	1	1	0	n
			1	1	1	0	1	1	0	0	1	0	1		$x^3 f(x)$
0	1	0	0	1	1	0	1	0	1	1	1	1			
		1	1	1	0	1	1	0	0	1	0	1			$x^2 f(x)$
0	1	1	1	0	1	1	0	0	1	0	1				
0	1	1	1	0	1	1	0	0	1	0	1				$x f(x)$

0

Polynom $g(x)=x^3+x^2+x$ je v tabulce 3 na 14. místě a prvek n je v tabulce 1 také na 14. místě. Tímto postupem jsme si ukázali správné dekódování přijatých slov.

Přijatá slova s nejvýše třemi chybami

Polynom $f(x)=1+x+x^2+x^4+x^5+x^8+x^{10}$ lze napsat jako součin tří polynomů a to:

$f_1(x)=x^4+x+1$

$f_3(x)=x^4+x^3+x^2+x+1$

$f_5(x)=x^2+x+1$

Přijaté slovo označíme jako $g(x)$.

Postup:

Nejprve spočítáme zbytky při dělení polynomu $g(x)$ polynomy $f_i(x)$. Tyto zbytky označíme $S_i(x)$. Dosadíme do $S_i(x)$ prvek α^i za prvek x. Nyní nám nic nebrání v tom, abychom dosadili do klíčové rovnice pro opravu chyb daného kódu, která má tvar $\left(S_1^3+S_3\right)y^3+\left(S_1^4+S_1S_3\right)y^2+\left(S_1^2S_3+S_5\right)y+S_1^6+S_1^3S_3+S_1S_5+S_3^2=0$.

Jestliže $S_1^3+S_3\neq 0$ a $\alpha^i,\alpha^j,\alpha^k$ jsou nenulové kořeny klíčové rovnice, potom se chyby v přijatém slově nacházejí na místech $i+1,\ j+1,k+1$, to znamená v koeficientech u x^i,x^j,x^k. Kořeny klíčové rovnice získáme po jednotlivém dosazování mocnin $1,\alpha,\alpha^2,\alpha^3,\ldots,\alpha^{14}$.

Je nutné si uvědomit, že počet chyb v přijatém slově je roven počtu kořenů klíčové rovnice.

Tento postup si ukážeme na příkladech.

Příklad 5.3

Byla přijata zpráva, která je tvořena řádky následující tabulky:

000011101100101

101111000100110

010111111110111

101111000100110

011110001001101

101100101000011.

Řešení:

$g(x) = 0\,0\,0\,0\,1\,1\,1\,0\,1\,1\,0\,0\,1\,0\,1$

$f(x) = 1 + x + x^2 + x^4 + x^5 + x^8 + x^{10}$

$$\begin{array}{cccccccccccccc} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ & & & & & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \end{array} \qquad x^4 f(x)$$

0

Polynom x^4 je v tabulce 3 na 16. místě stejně jako prvek p v tabulce 1.

$g(x) = 1\,0\,1\,1\,1\,1\,0\,0\,1\,0\,0\,1\,1\,0$

$f(x) = 1 + x + x^2 + x^4 + x^5 + x^8 + x^{10}$

$$\begin{array}{cccccccccccccc} 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ & & & & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \end{array} \qquad x^3 f(x)$$

$$\begin{array}{cccccccccccccc} 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & & \\ & & & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & \end{array} \qquad x^2 f(x)$$

$$\begin{array}{cccccccccccccc} 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & & & \\ & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & & & \end{array} \qquad x\, f(x)$$

$$\begin{array}{cccccccccccccc} 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & & & & \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & & & & \end{array} \qquad f(x)$$

0

Polynom $x^3 + x^2 + x + 1$ je v tabulce 3 na 15. místě stejně jako prvek o v tabulce 1.

$g(x) = 0\,1\,0\,1\,1\,1\,1\,1\,1\,1\,1\,0\,1\,1\,1$

$f(x)=1+x+x^2+x^4+x^5+x^8+x^{10}$

0 1 0 1 1 1 1 1 1 1 1 0 1 1 1

1 1 1 0 1 1 0 0 1 0 1 $\quad x^4 f(x)$

---

0 1 0 1 0 0 0 1 0 0 1 0 0 1 0

1 1 1 0 1 1 0 0 1 0 1 $\quad x^3 f(x)$

---

0 1 0 0 1 1 0 0 1 0 1 1 0 0

1 1 1 0 1 1 0 0 1 0 1 $\quad x\ f(x)$

---

0 0 1 1 1 0 1 0 1 1 1 0

1 1 1 0 1 1 0 0 1 0 1 $\quad f(x)$

---

1 1 0 1 0 1 1 0 0 1 0

Přijaté slovo není dělitelné polynomem $f(x)=1+x+x^2+x^4+x^5+x^8+x^{10}$ a proto toto přijaté slovo není kódové slovo. Z toho vyplývá, že při přenosu zprávy došlo u tohoto prvku k chybě. V takovém případě polynom $g(x)$ vydělíme $f_1(x)=x^4+x+1$.

0 1 0 1 1 1 1 1 1 1 1 0 1 1 1

1 1 0 0 1

---

0 1 0 1 1 1 1 1 1 1 0 1 1 1 0

1 1 0 0 1

---

0 1 0 1 1 1 1 1 1 0 1 1 1 0

1 1 0 0 1

---

0 1 0 1 1 1 1 1 0 1 1 1 0

1 1 0 0 1

---

0 1 0 1 1 1 1 0 1 1 1 0

1 1 0 0 1

---

0 1 0 1 1 1 0 1 1 1 0

1 1 0 0 1

---

0 1 0 1 1 0 1 1 1 0
1 1 0 0 1

0 1 0 1 0 1 1 1 0
1 1 0 0 1

0 1 0 0 1 1 1 0
1 1 0 0 1

0 1 1 1 1 1 0
1 1 0 0 1

0 0 0 1 1 0
1 1 0 0 1

1 1 0 1 0

Dostaneme zbytek $11010 \Rightarrow 1+x+x^3$. Zbytek S_1 získáme po dosazení prvku α za prvek x, dle tabulky 2. $S_1 = 1+x+x^3 = \alpha^3+\alpha+1 = \alpha^7$.

Nyní polynom $g(x)$ vydělíme polynomem $f_3(x) = x^4+x^3+x^2+x+1$

0 1 0 1 1 1 1 1 1 1 1 0 1 1 1
1 1 1 1 1

0 1 0 1 1 1 1 1 1 1 0 1 0 0 0
1 1 1 1 1

0 1 0 1 1 1 1 0 0 0 1 0
1 1 1 1 1

0 1 0 1 1 1 0 1 1 1 0
1 1 1 1 1

0 1 0 1 1 0 1 0 0 0
1 1 1 1 1

0 1 1 0 0 1 0
1 1 1 1 1

$$\begin{array}{cccccc} 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & \\ \hline 1 & 1 & 1 & 0 & 0 & \end{array}$$

Dostaneme zbytek $11100 \Rightarrow 1+x+x^2$, po dosazení prvku α za prvek x dostaneme S_3, dle tabulky 2. $S_3 = x + x^2 = \alpha^2 + \alpha = \alpha^8$.

Dále polynom $g(x)$ vydělíme polynomem $f_5(x) = x^2 + x + 1$.

$$\begin{array}{cccccccccccccc} 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ & & & & & & & & & & & & 1 & 1 & 1 \\ \hline 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ & & & & & & & & & & & & 1 & 1 & 1 \\ \hline 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ & & & & & & & & & 1 & 1 & 1 & & & \\ \hline 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & & & & \\ & & & & & & & 1 & 1 & 1 & & & & & \\ \hline 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & & & & & & & \\ & & & 1 & 1 & 1 & & & & & & & & & \\ \hline 0 & 1 & 1 & 0 & 0 & & & & & & & & & & \\ 1 & 1 & 1 & & & & & & & & & & & & \\ \hline 1 & 0 & 0 & & & & & & & & & & & & \end{array}$$

Dostaneme zbytek $100 \Rightarrow 1$, tím jsme získali $S_5 = 1$.

Nyní jsme zjistili potřebné zbytky polynomů do klíčové rovnice a přejdeme k výpočtu, tím že dosadíme do rovnice $\left(S_1^3 + S_3\right)y^3 + \left(S_1^4 + S_1 S_3\right)y^2 + \left(S_1^2 S_3 + S_5\right)y +$

$+S_1^6 + S_1^3 S_3 + S_1 S_5 + S_3^2 = 0$.

$S_1^3 + S_3 = \left(\alpha^7\right)^3 + \alpha^8 = \alpha^{21} + \alpha^8 = \alpha^{15} \cdot \alpha^6 + \alpha^8 = 1 \cdot \alpha^6 + \alpha^8 = \alpha^3 + \alpha^2 + \alpha^2 + 1 = \alpha^3 + 1 = \alpha^{14}$

$S_1^4 + S_1 S_3 = \left(\alpha^7\right)^4 + \alpha^7 \alpha^8 = \alpha^{28} + \alpha^{15} = 1 \cdot \alpha^{13} + 1 = \alpha^3 + \alpha^2 + 1 + 1 = \alpha^3 + \alpha^2 = \alpha^6$

$S_1^2 S_3 + S_5 = \left(\alpha^7\right)^2 \alpha^8 + 1 = \alpha^{14}\alpha^8 + 1 = 1 \cdot \alpha^7 + 1 = \alpha^3 + \alpha + 1 + 1 = \alpha^3 + \alpha = \alpha^9$

$S_1^6 + S_1^3 S_3 + S_1 S_5 + S_3^2 = \left(\alpha^7\right)^6 + \left(\alpha^7\right)^3 \alpha^8 + \alpha^7 \cdot 1 + \left(\alpha^8\right)^2 = \alpha^{42} + \alpha^{21}\alpha^8 + \alpha^7 + \alpha^{16} = \alpha^{12} +$

$+ \alpha^{14} + \alpha^7 + \alpha = \alpha^3 + \alpha^2 + \alpha + 1 + \alpha^3 + 1 + \alpha^3 + \alpha + 1 + \alpha = \alpha^3 + \alpha^2 + \alpha + 1 = \alpha^{12}$.

Klíčová rovnice je tedy $\alpha^{14} y^3 + \alpha^6 y^2 + \alpha^9 y + \alpha^{12} = 0$.

Rovnici vynásobíme α a tedy získáme $\alpha^{15} y^3 + \alpha^7 y^2 + \alpha^{10} y + \alpha^{13} = 0 \Rightarrow y^3 + \alpha^7 y^2 +$

$+\alpha^{10} y + \alpha^{13} = 0$. Nyní budeme dosazovat postupně mocniny $1, \alpha, \alpha^2, \ldots, \alpha^{14}$.

1: $1 + \alpha^7 + \alpha^{10} + \alpha^{13} = 1 + \alpha^3 + \alpha + 1 + \alpha^2 + \alpha + 1 + \alpha^3 + \alpha^2 + 1 = 0$

α: $\alpha^3 + \alpha^9 + \alpha^{11} + \alpha^{13} = \alpha^3 + \alpha^3 + \alpha + \alpha^3 + \alpha^2 + \alpha + \alpha^3 + \alpha^2 + 1 = 1$

α^2: $\alpha^6 + \alpha^{11} + \alpha^{12} + \alpha^{13} = \alpha^3 + \alpha^2 + \alpha^3 + \alpha^2 + \alpha + \alpha^3 + \alpha^2 + \alpha + 1 + \alpha^3 + \alpha^2 + 1 = 0$

α^3: $\alpha^{24} + \alpha^{13} + \alpha^{13} + \alpha^{13} = \alpha^9 + \alpha^{13} + \alpha^{13} + \alpha^{13} = \alpha^3 + \alpha + \alpha^3 + \alpha^2 + 1 + \alpha^3 + \alpha^2 + 1 +$

$+\alpha^3 + \alpha^2 + 1 = \alpha^2 + \alpha + 1 = \alpha^{10}$

α^4: $\alpha^{12} + \alpha^{15} + \alpha^{14} + \alpha^{13} = \alpha^3 + \alpha^2 + \alpha + 1 + 1 + \alpha^3 + 1 + \alpha^3 + \alpha^2 + 1 = \alpha^3 + \alpha = \alpha^9$

α^5: $\alpha^{15} + \alpha^{17} + \alpha^{15} + \alpha^{13} = 1 + \alpha^2 + 1 + \alpha^{13} = 1 + \alpha^2 + 1 + \alpha^3 + \alpha^2 + 1 = \alpha^3 + 1 = \alpha^{14}$

α^6: $\alpha^{18} + \alpha^{19} + \alpha^{16} + \alpha^{13} = \alpha^3 + \alpha^4 + \alpha + \alpha^{13} = \alpha^3 + \alpha + 1 + \alpha + \alpha^3 + \alpha^2 + 1 = \alpha^2$

α^7: $\alpha^{21} + \alpha^{21} + \alpha^{17} + \alpha^{13} = \alpha^6 + \alpha^6 + \alpha^2 + \alpha^{13} = \alpha^3 + \alpha^2 + \alpha^3 + \alpha^2 + \alpha^2 + \alpha^3 + \alpha^2 + 1 =$

$= \alpha^3 + 1 = \alpha^{14}$

α^8: $\alpha^{24} + \alpha^{23} + \alpha^{18} + \alpha^{13} = \alpha^9 + \alpha^8 + \alpha^3 + \alpha^{13} = \alpha^3 + \alpha + \alpha^2 + 1 + \alpha^3 + \alpha^3 + \alpha^2 + 1 = \alpha^3 +$

$+\alpha = \alpha^9$

α^9: $\alpha^{27} + \alpha^{25} + \alpha^{19} + \alpha^{13} = \alpha^{12} + \alpha^{10} + \alpha^4 + \alpha^{13} = \alpha^3 + \alpha^2 + \alpha + 1 + \alpha^2 + \alpha + 1 + \alpha + 1 +$

$+\alpha^3 + \alpha^2 + 1 = \alpha^2 + \alpha = \alpha^5$

α^{10}: $\alpha^{30} + \alpha^{27} + \alpha^{20} + \alpha^{13} = 1 + \alpha^{12} + \alpha^5 + \alpha^{13} = 1 + \alpha^3 + \alpha^2 + \alpha + 1 + \alpha^2 + \alpha + \alpha^3 + \alpha^2 +$

$+1 = \alpha^2 + 1 = \alpha^8$

α^{11}: $\alpha^{33} + \alpha^{29} + \alpha^{21} + \alpha^{13} = \alpha^3 + \alpha^{14} + \alpha^6 + \alpha^{13} = \alpha^3 + \alpha^3 + 1 + \alpha^3 + \alpha^2 + \alpha^3 + \alpha^2 + 1 = 0$

α^{12}: $\alpha^{36} + \alpha^{31} + \alpha^{22} + \alpha^{13} = \alpha^6 + \alpha + \alpha^7 + \alpha^{13} = \alpha^3 + \alpha^2 + \alpha + \alpha^3 + \alpha + 1 + \alpha^3 + \alpha^2 + 1 =$

$= \alpha^3$

α^{13}: $\alpha^{39} + \alpha^{33} + \alpha^{23} + \alpha^{13} = \alpha^9 + \alpha^3 + \alpha^8 + \alpha^{13} = \alpha^3 + \alpha + \alpha^3 + \alpha^2 + 1 + \alpha^3 + \alpha^2 + 1 =$

$$= \alpha^3 + \alpha = \alpha^9$$

$$\alpha^{14}: \quad \alpha^{42} + \alpha^{35} + \alpha^{24} + \alpha^{13} = \alpha^{12} + \alpha^5 + \alpha^9 + \alpha^{13} = \alpha^3 + \alpha^2 + \alpha + 1 + \alpha^2 + \alpha + \alpha^3 + \alpha +$$
$$+ \alpha^3 + \alpha^2 + 1 = \alpha^3 + \alpha^2 + \alpha = \alpha^{11}.$$

Dostáváme pro 1 rovnost $1 + \alpha^7 + \alpha^{10} + \alpha^{13} = 0$, pro α^2 rovnost $\alpha^6 + \alpha^{11} + \alpha^{12} + \alpha^{13} = 0$ a pro α^{11} rovnost $\alpha^3 + \alpha^{14} + \alpha^6 + \alpha^{13} = 0$. Proto klíčová rovnice má kořeny 1, α^2 a α^{11}, tudíž chyby jsou tedy na 1., 3. a 12. místě. Správně přijaté slovo mělo být 111111111111111.

Toto slovo vydělíme polynomem $f(x) = 1 + x + x^2 + x^4 + x^5 + x^8 + x^{10}$.

1 1 1 1 1 1 1 1 1 1 1 1 1 1 1

1 1 1 0 1 1 0 0 1 0 1 $\quad x^4 f(x)$

1 1 1 1 0 0 0 1 0 0 1 1 0 1 0

1 1 1 0 1 1 0 0 1 0 1 $\quad x^3 f(x)$

1 1 1 0 1 1 0 0 1 0 1 0 0 0

1 1 1 0 1 1 0 0 1 0 1 $\quad f(x)$

0

Polynom $x^4 + x^3 + 1$ je v tabulce 3 na 25. místě stejně jako prvek z v tabulce 1.

$$g(x) = 101111000100110$$

$$f(x) = 1 + x + x^2 + x^4 + x^5 + x^8 + x^{10}$$

Tento postup počítat nebudeme, protože polynom $g(x)$ je stejný jako v druhém řádku v zadané tabulce. Tudíž bychom dostali stejný polynom $x^3 + x^2 + x + 1$, který je v tabulce 3 na 15. místě stejně jako prvek o v tabulce 1.

$$g(x) = 011110001001101$$

$$f(x) = 1 + x + x^2 + x^4 + x^5 + x^8 + x^{10}$$

$$\begin{array}{ccccccccccccccc} 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ & & & & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ \hline 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & & & \\ & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & & & \\ \hline 0 & & & & & & & & & & & & & & \end{array} \qquad \begin{array}{l} x^4 f(x) \\ \\ x f(x) \end{array}$$

Polynom $x^4 + x$ je v tabulce 3 na 18. místě stejně jako prvek r v tabulce 1.

$g(x) = 1011001010000 11$

$f(x) = 1 + x + x^2 + x^4 + x^5 + x^8 + x^{10}$

$$\begin{array}{ccccccccccccccc} 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ & & & & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ \hline 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & \\ & & & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & \\ \hline 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & & \\ & & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & & \\ \hline 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & & & \\ & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & & & \\ \hline 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & & & & \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & & & & \\ \hline 0 & & & & & & & & & & & & & & \end{array} \qquad \begin{array}{l} x^4 f(x) \\ \\ x^3 f(x) \\ \\ x^2 f(x) \\ \\ x f(x) \\ \\ f(x) \end{array}$$

Polynom $x^4 + x^3 + x^2 + x + 1$ je v tabulce 3 na 31. místě stejně jako prvek ! v tabulce 1.

Výsledný text je *POZOR*!.

Příklad 5.4

Přijali jsme zprávu, která je tvořena řádky následující tabulky:

000011101100101

101111000100110

000111011001010

101111000100110

010100111001001

100001110110010

110011011010000.

Řešení:

$g(x) = 0\,0\,0\,0\,1\,1\,1\,0\,1\,1\,0\,0\,1\,0\,1$

$f(x) = 1 + x + x^2 + x^4 + x^5 + x^8 + x^{10}$

$$\begin{array}{cccccccccccccccc} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & \\ & & & & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & x^4 f(x) \\ \hline 0 & & & & & & & & & & & & & & & \end{array}$$

Polynom x^4 je v tabulce 3 na 16. místě stejně jako prvek p v tabulce 1.

$g(x) = 1\,0\,1\,1\,1\,1\,0\,0\,1\,0\,0\,1\,1\,0$

$f(x) = 1 + x + x^2 + x^4 + x^5 + x^8 + x^{10}$

$$\begin{array}{cccccccccccccccc} 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & \\ & & & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & & x^3 f(x) \\ \hline 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & & & \\ & & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & & & x^2 f(x) \\ \hline 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & & & & \\ & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & & & & x f(x) \\ \hline 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & & & & & \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & & & & & f(x) \\ \hline 0 & & & & & & & & & & & & & & & \end{array}$$

Polynom $x^3 + x^2 + x + 1$ je v tabulce 3 na 15. místě stejně jako prvek o v tabulce 1.

$g(x) = 0\,0\,0\,1\,1\,1\,0\,1\,1\,0\,0\,1\,0\,1\,0$

$f(x) = 1 + x + x^2 + x^4 + x^5 + x^8 + x^{10}$

$$\begin{array}{cccccccccccccc} 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ & & & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & \end{array} \qquad x^3 f(x)$$

0

Polynom x^3 je v tabulce 3 na 8. místě stejně jako prvek h v tabulce 1.

$g(x) = 1\,0\,1\,1\,1\,1\,0\,0\,0\,1\,0\,0\,1\,1\,0$

$f(x) = 1 + x + x^2 + x^4 + x^5 + x^8 + x^{10}$

Tento postup počítat nebudeme, protože polynom $g(x)$ je stejný jako v druhém řádku v zadané tabulce. Tudíž bychom dostali stejný polynom $x^3 + x^2 + x + 1$, který je v tabulce 3 na 15. místě stejně jako prvek o v tabulce 1.

$g(x) = 0\,1\,0\,0\,0\,0\,1\,1\,1\,0\,1\,1\,0\,0\,1$

$f(x) = 1 + x + x^2 + x^4 + x^5 + x^8 + x^{10}$

$$\begin{array}{cccccccccccccc} 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ & & & & & & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & \end{array} \qquad x^4 f(x)$$

$$\begin{array}{cccccccccccccc} 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ & & & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & & & & \end{array} \qquad x^2 f(x)$$

$$\begin{array}{cccccccccccccc} 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & & & & \end{array} \qquad x f(x)$$

0

Polynom $x^4 + x^2 + x$ je v tabulce 3 na 22. místě stejně jako prvek v v tabulce 1.

$g(x) = 1\,0\,0\,0\,0\,1\,1\,1\,0\,1\,1\,0\,0\,1\,0$

$f(x)=1+x+x^2+x^4+x^5+x^8+x^{10}$

1 0 0 0 0 1 1 1 0 1 1 0 0 1 0

1 1 1 0 1 1 0 0 1 0 1 $\qquad x^3 f(x)$

1 0 0 1 1 0 1 0 1 1 1 1 0 0

1 1 1 0 1 1 0 0 1 0 1 $\qquad x f(x)$

1 1 1 0 1 1 0 0 1 0 1 0

1 1 1 0 1 1 0 0 1 0 1 $\qquad f(x)$

0

Polynom x^3+x+1 je v tabulce 3 na 11. místě stejně jako prvek k v tabulce 1.

$g(x)=110011011010000$

$f(x)=1+x+x^2+x^4+x^5+x^8+x^{10}$

1 1 0 0 1 1 0 1 1 0 1 0 0 0 0

1 1 1 0 1 1 0 0 1 0 1 $\qquad x\ f(x)$

0 0 1 0 0 0 0 1 0 0 0

Přijaté slovo není dělitelné polynomem $f(x)=1+x+x^2+x^4+x^5+x^8+x^{10}$ a přijaté slovo není proto kódové slovo. Z toho vyplývá, že při přenosu zprávy došlo u tohoto prvku k chybě. V takovém případě polynom $g(x)$ vydělíme $f_1(x)=x^4+x+1$.

1 1 0 0 1 1 0 1 1 0 1 0 0 0 0

1 1 0 0 1

1 1 0 0 1 1 1 0 1 0 0

1 1 0 0 1

1 1 0 0 0 0 1 0 0

1 1 0 0 1

1 1 1 1 0 0 0

Dostaneme zbytek $1111 \Rightarrow 1+x+x^2+x^3$. Zbytek S_1 získáme po dosazení prvku α za prvek x, dle tabulky 2. $S_1 = 1+x+x^2+x^3 = \alpha^3+\alpha^2+\alpha+1 = \alpha^{12}$.

Nyní polynom $g(x)$ vydělíme polynomem $f_3(x) = x^4+x^3+x^2+x+1$.

1 1 0 0 1 1 0 1 1 0 1 0 0 0 0
      1 1 1 1 1
---
1 1 0 0 1 1 1 0 0 1 0
     1 1 1 1 1
---
1 1 0 0 1 0 0 1 1 0
    1 1 1 1 1
---
1 1 0 0 0 1 1 0 0
  1 1 1 1 1
---
1 1 1 1 1 0 0
1 1 1 1 1

0

Dostaneme zbytek $00000 \Rightarrow 0$. Zbytek S_3 získáme po dosazení prvku α za prvek x, dle tabulky 2. $S_3 = 0$.

Dále polynom $g(x)$ vydělíme polynomem $f_5(x) = x^2+x+1$.

1 1 0 0 1 1 0 1 1 0 1 0 0 0 0
        1 1 1
---
1 1 0 0 1 1 0 1 0 1 0
       1 1 1
---
1 1 0 0 1 1 0 0 1 0
     1 1 1
---
1 1 0 0 1 1 1 1 0
    1 1 1
---

1 1 0 0 1 0 0 0

1 1 1

---

1 1 1 1 0

1 1 1

---

1 0 0 0

Dostaneme zbytek $1000 \Rightarrow 1$, tím jsme získali $S_5 = 1$.

Nyní jsme zjistili potřebné zbytky do klíčové rovnice a přejdeme k výpočtu, tím že dosadíme do rovnice ve tvaru:

$$\left(S_1^3 + S_3\right) y^3 + \left(S_1^4 + S_1 S_3\right) y^2 + \left(S_1^2 S_3 + S_5\right) y + S_1^6 + S_1^3 S_3 + S_1 S_5 + S_3^2 = 0.$$

$$S_1^3 + S_3 = \left(\alpha^{12}\right)^3 + 0 = \left(\alpha^{15}\right)^3 \cdot \alpha^6 = 1 \cdot \alpha^6 = \alpha^6$$

$$S_1^4 + S_1 S_3 = \left(\alpha^{12}\right)^4 + \alpha^{12} \cdot 0 = \left(\alpha^{15}\right)^3 \alpha^3 + 0 = \alpha^3 + 0 = \alpha^3$$

$$S_1^2 S_3 + S_5 = \left(\alpha^{12}\right)^2 \cdot 0 + 1 = \alpha^{24} \cdot 0 + 1 = 1$$

$$S_1^6 + S_1^3 S_3 + S_1 S_5 + S_3^2 = \left(\alpha^{12}\right)^6 + \left(\alpha^{12}\right)^3 \cdot 0 + \alpha^{12} \cdot 1 + \left(0\right)^2 = \left(\alpha^{15}\right)^4 \alpha^{12} + 0 + \alpha^{12} + 0 = \alpha^{12} + \alpha^{12} = 0.$$

Klíčová rovnice je tedy $\alpha^6 y^3 + \alpha^3 y^2 + y + 0 = 0$.

Rovnici zkrátíme y vynásobíme α^9 a tedy získáme $\alpha^{15} y^2 + \alpha^{12} y + \alpha^9 = 0 \Rightarrow y^2 + \alpha^{12} y +$

$+\alpha^9 = 0$. Nyní budeme dosazovat postupně mocniny $1, \alpha, \alpha^2, \ldots, \alpha^{14}$.

1: $1 + \alpha^{12} + \alpha^9 = \alpha^3 + \alpha^2 + \alpha + 1 + \alpha^3 + \alpha = \alpha^2 + 1 = \alpha^8$

α: $\alpha^2 + \alpha^{13} + \alpha^9 = \alpha^2 + \alpha^3 + \alpha^2 + 1 + \alpha^3 + \alpha = \alpha + 1 = \alpha^4$

α^2: $\alpha^4 + \alpha^{14} + \alpha^9 = \alpha + 1 + \alpha^3 + 1 + \alpha^3 + \alpha = 0$

α^3: $\alpha^6 + \alpha^{15} + \alpha^9 = \alpha^3 + \alpha^2 + 1 + \alpha^3 + \alpha = \alpha^2 + \alpha + 1 = \alpha^{10}$

α^4: $\alpha^8 + \alpha^{16} + \alpha^9 = \alpha^2 + 1 + \alpha + \alpha^3 + \alpha = \alpha^3 + \alpha^2 + 1 = \alpha^{13}$

α^5: $\alpha^{10} + \alpha^{17} + \alpha^9 = \alpha^{10} + \alpha^2 + \alpha^9 = \alpha^2 + \alpha + 1 + \alpha^2 + \alpha^3 + \alpha = \alpha^3 + 1 = \alpha^{14}$

α^6: $\alpha^{12} + \alpha^{18} + \alpha^9 = \alpha^{12} + \alpha^3 + \alpha^9 = \alpha^3 + \alpha^2 + \alpha + 1 + \alpha^3 + \alpha^3 + \alpha = \alpha^3 + \alpha^2 + 1 = \alpha^{13}$

α^7: $\alpha^{14} + \alpha^{19} + \alpha^9 = \alpha^{14} + \alpha^4 + \alpha^9 = \alpha^3 + 1 + \alpha + 1 + \alpha^3 + \alpha = 0$

$\alpha^8:\quad \alpha^{16}+\alpha^{20}+\alpha^9=\alpha+\alpha^5+\alpha^9=\alpha+\alpha^2+\alpha+\alpha^3+\alpha=\alpha^3+\alpha^2+\alpha=\alpha^{11}$

$\alpha^9:\quad \alpha^{18}+\alpha^{21}+\alpha^9=\alpha^3+\alpha^6+\alpha^9=\alpha^3+\alpha^3+\alpha^2+\alpha^3+\alpha=\alpha^3+\alpha^2+\alpha=\alpha^{11}$

$\alpha^{10}:\quad \alpha^{20}+\alpha^{22}+\alpha^9=\alpha^5+\alpha^7+\alpha^9=\alpha^2+\alpha+\alpha^3+\alpha+1+\alpha^3+\alpha=\alpha^2+\alpha+1=\alpha^{10}$

$\alpha^{11}:\quad \alpha^{22}+\alpha^{23}+\alpha^9=\alpha^7+\alpha^8+\alpha^9=\alpha^3+\alpha+1+\alpha^2+1+\alpha^3+\alpha=\alpha^2$

$\alpha^{12}:\quad \alpha^{24}+\alpha^{24}+\alpha^9=\alpha^9+\alpha^9+\alpha^9=\alpha^9$

$\alpha^{13}:\quad \alpha^{26}+\alpha^{25}+\alpha^9=\alpha^{11}+\alpha^{10}+\alpha^9=\alpha^3+\alpha^2+\alpha+\alpha^2+\alpha+1+\alpha^3+\alpha=\alpha+1=\alpha^4$

$\alpha^{14}:\quad \alpha^{28}+\alpha^{26}+\alpha^9=\alpha^{13}+\alpha^{11}+\alpha^9=\alpha^3+\alpha^2+1+\alpha^3+\alpha^2+\alpha+\alpha^3+\alpha=\alpha^3+1=\alpha^{14}$

Dostáváme pro α^2 rovnost $\alpha^4+\alpha^{14}+\alpha^9=0$ a pro α^7 rovnost $\alpha^{14}+\alpha^4+\alpha^9=0$. Proto klíčová rovnice má kořeny α^2 a α^7, tudíž chyby jsou na 3. a 8. místě. Správně přijaté slovo mělo být 111011001010000.

Toto slovo vydělíme polynomem $f(x)=1+x+x^2+x^4+x^5+x^8+x^{10}$.

1 1 1 0 1 1 0 0 1 0 1 0 0 0 0

1 1 1 0 1 1 0 0 1 0 1 $\qquad f(x)$

0

Polynom 1 je v tabulce 3 na 1. místě stejně jako prvek a v tabulce 1. Výsledný text je *POHOVKA*.

6. HAMMINGŮV KÓD

Richard W. Hamming

První samoopravné kódy navrhnul americký matematik Richard W. Hamming krátce po druhé světové válce. Jeho návrh spočíval v kombinaci několika testů na paritu. V roce 1968 R. Hamming získal cenu A. M. Turinga za přínos v oboru informatiky (numerické metody, systémy automatického kódování, kódy pro detekci a opravu chyb).

Tento kód je binární, jestliže má kontrolní matici, jejíž sloupce jsou všechna nenulová slova dané délky $n-k=r$ a žádné z nich se neopakuje. Jedná se o speciální případ lineárních dvojkových (n,k) kódů. Tyto kódy opravují jednu chybu při vzdálenosti kódových slov $d_{\min}(b_i,b_j)=3$ a v rozšířené variantě $d_{\min}(b_i,b_j)=4$.

Algoritmus generování Hammingova kódu

Všechny bitové pozice, jejichž číslo je rovné druhé mocnině jsou použity pro paritní bit $(1,2,4,8,16,32,\ldots)$.

Všechny ostatní bitové pozice náleží kódovanému informačnímu slovu $(3,5,6,7,9,10,11,12,13,14,15,17,\ldots)$.

Každý paritní bit je vypočítán z některých bitů informačního slova. Pozice paritního bitu udává sekvenci bitů, které jsou v kódovém slově zjišťovány a některé přeskočeny. Pro paritní bit p_1 (pozice 1) se ve zbylém kódovém slově 1 bit přeskočí, 1 zkontroluje, 1 bit přeskočí, 1 zkontroluje, atd. Pro paritní bit p_2 (pozice 2) přeskočí první bit, 2 zkontroluje, 2 přeskočí, 2 zkontroluje, atd. Pro p_3 (pozice 4) přeskočí první 3 bity, 4 zkontroluje, 4 přeskočí, 4 zkontroluje, atd.

Pro kód $(7,4)$ platí $b=\left(p_1^{(2^0)}, p_2^{(2^1)}\, a_1^3, p_3^{(2^2)}, a_2^5, a_3^6, a_4^7\right)$:

$p_1+a_1+a_2+a_4=0$ podle bodu 3 sestaveno z (b_1,b_3,b_5,b_7),

$p_2+a_1+a_3+a_4=0$ (b_2,b_3,b_6,b_7),

$p_3+a_2+a_3+a_4=0$ (b_4,b_5,b_6,b_7).

Generující matice G Hammingova kódu $(7,4)$ se sestrojí tak, že se postupně zakóduje posloupnost $1000_1, 0100_2, 0010_3, 0001_4$, aby řádky byly lineárně nezávislé a tvořily bázi prostoru.

$$G=\begin{pmatrix} & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & p_{1_1} & p_{2_1} & 1 & p_{3_1} & 0 & 0 & 0 \\ 2 & p_{1_2} & p_{2_2} & 0 & p_{3_2} & 1 & 0 & 0 \\ 3 & p_{1_3} & p_{2_3} & 0 & p_{3_3} & 0 & 1 & 0 \\ 4 & p_{1_4} & p_{2_4} & 0 & p_{3_4} & 0 & 0 & 1 \end{pmatrix}=\begin{pmatrix} & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 2 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 3 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 4 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

Kontrolní matice H kódu $(7,4)$ se určí následovně. Po přijetí kódového slova b víme, že bity b_3, b_5, b_6, b_7, obsahují informační slovo a zbylé redundantní bity jsou určeny tak, aby

$s_1 = b_4 + b_5 + b_6 + b_7 = 0$, $s_2 = b_2 + b_3 + b_6 + b_7 = 0$, $s_3 = b_1 + b_3 + b_5 + b_7 = 0 \Rightarrow H$

$$H=\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

Vektor $s=(s_1, s_2, s_3)$ se nazývá syndrom a pokud byla informace přijata bezchybně jeho hodnota je $s=(0,0,0)$.

Rozšíření binárního Hammingova kódu vychází z toho, že přidáme na začátek každého kódového slova nový symbol určený pro kontrolu parity celého kódového slova. Bit p_0 je zvolen tak, aby $p_0 + b_1 + b_2 + b_3 + b_4 + b_5 + b_6 + b_7$ vycházelo jako sudé číslo. Rozšířený kód dovoluje, tak jako předchozí opravit jednu chybu a navíc je schopen detekovat dvě chyby.

Generující matice $G´$ rozšířeného kódu $(8,4)$ se sestrojí tak, že se postupně zakóduje posloupnost $1000_1, 0100_2, 0010_3, 0001_4$.

$$G´=\begin{pmatrix} p_{0_1} & p_{1_1} & p_{2_1} & 1 & p_{3_1} & 0 & 0 & 0 \\ p_{0_2} & p_{1_2} & p_{2_2} & 0 & p_{3_2} & 1 & 0 & 0 \\ p_{0_3} & p_{1_3} & p_{2_3} & 0 & p_{3_3} & 0 & 1 & 0 \\ p_{0_4} & p_{1_4} & p_{2_4} & 0 & p_{3_4} & 0 & 0 & 1 \end{pmatrix}=\begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

Dekódování a kontrola

Nejprve se po přijetí kódového slova b určí syndrom $s = H \cdot b^T$. Uvedeme si například přijaté slovo $b = (1010111)$ a jeho syndrom je

$$s = H \cdot b^T = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \end{pmatrix} =$$

$$= \begin{pmatrix} 0+0+0+0+1+1+1 \\ 0+0+1+0+0+1+1 \\ 1+0+1+0+1+0+1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}.$$

Vidíme, že syndrom s je nenulový, tudíž při přenosu došlo k chybě. Syndrom, který jsme zjistili $s = (1,1,0)$ odpovídá šestému sloupci kontrolní matice H. Z tohoto syndromu lze poznat chybu, kterou je třeba opravit v šestém bitu kódového slova $b_0 = (1010101)$.

Nyní si ukážeme případ tohoto kódu, který se označuje (7, 4, 3). Tento kód má čtyři informační a tři kontrolní cifry, jeho délka je tedy 7. Kontrolní cifry jsou na prvním, druhém a čtvrtém místě kódového slova, informační cifry jsou na místech 3,5,6,7. Nejdříve si místa cifer ve slově vyjádříme ve dvojkové soustavě:

1 = 001
2 = 010
3 = 011
4 = 100
5 = 101
6 = 110
7 = 111

Jsou-li nyní dány informační cifry a_3, a_5, a_6, a_7 potřebujeme v kódovém slově a_3, a_5, a_6, a_7 dopočítat kontrolní cifry a_1, a_2, a_4. Kontrolní cifra a_1 zajistí, aby byl v kódovém slově sudý počet cifer 1 na místech, která mají ve dvojkovém vyjádření

jednotku na místě jednotek, tj. vpravo. To znamená, že $a_1 + a_3 + a_5 + a_7 = 0$, neboli $a_1 = a_3 + a_5 + a_7$. Podobně kontrolní cifra a_2 zajistí, aby byl v každém kódovém slově sudý počet cifer 1 na místech, která mají ve dvojkovém vyjádření jednotku namístě desítek, tj. uprostřed. Proto $a_2 + a_3 + a_6 + a_7 = 0$, neboli $a_2 = a_3 + a_6 + a_7$. A nakonec dopočítáme kontrolní cifru a_4 tak, aby byl v každém slově sudý počet cifer 1 na místech, která mají ve dvojkovém vyjádření jednotku na místě stovek, tj. vlevo: $a_4 + a_5 + a_6 + a_7 = 0$, neboli $a_4 = a_5 + a_6 + a_7$.

Ve všech třech rovnostech je vždy jediná kontrolní cifra a zbývající tři jsou informační. Každá rovnost tak umožňuje jednoznačně vypočítat kontrolní cifru. Každé kódové slovo $a_1\, a_2\, a_3\, a_4\, a_5\, a_6\, a_7$ Hammingova kódu H je tak řešením následující soustavy tří rovnic o sedmi neznámých nad dvouprvkovým tělesem Z_2:

$a_1 + a_3 + a_5 + a_7 = 0$

$a_2 + a_3 + a_6 + a_7 = 0$

$a_4 + a_5 + a_6 + a_7 = 0$.

A naopak, každé řešení této soustavy je prvkem kódu H. Hammingův kód tak můžeme definovat jako množinu všech řešení této soustavy.

$$H = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Matice této homogenní soustavy má hodnost 3, protože je v redukovaném řádkově odstupňovaném tvaru. Nyní si ukážeme, jak lze pomocí Hammingova kódu odhalit a opravit jednu chybu. Pokud přijmeme slovo $b_1\, b_2\, b_3\, b_4\, b_5\, b_6\, b_7$, dosadíme cifry $b_1, b_2, b_3, b_4, b_5, b_6, b_7$ do rovnic definujících Hammingův kód a spočítáme čísla vektoru $s = (s_1, s_2, s_3), s_1, s_2, s_3 \in Z_2$.

$b_1 + b_3 + b_5 + b_7 = s_1$

$b_2 + b_3 + b_6 + b_7 = s_2$

$b_4 + b_5 + b_6 + b_7 = s_3$.

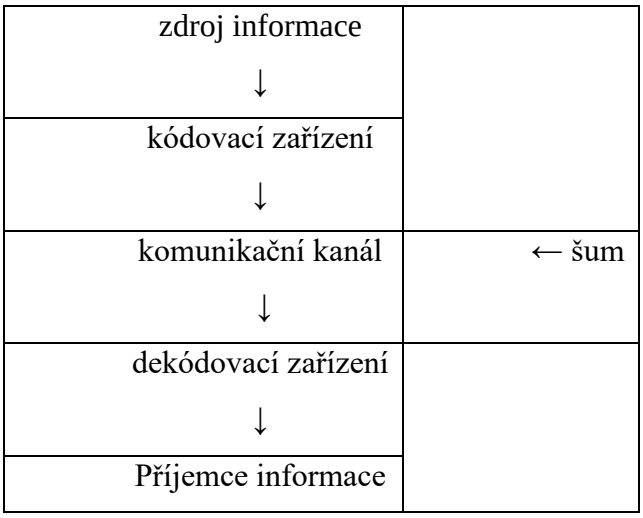
Pokud je $s_1 = s_2 = s_3 = 0$, je slovo $b_1\, b_2\, b_3\, b_4\, b_5\, b_6\, b_7$ kódovým slovem. Pokud je aspoň jedno z čísel s_1, s_2, s_3 různé od 0, tak při přenosu došlo k chybě. Je-li $s_1 = 1$, pak k chybě došlo na některém z míst, která mají ve vyjádření ve dvojkové soustavě 1 na místě jednotek, tj. u jedné z cifer b_1, b_3, b_5, b_7. Je-li rovněž $s_2 = 1$, pak je chyba také u jedné z cifer na místech, která mají ve dvojkové soustavě 1 na místě desítek, tj. u cifer b_2, b_3, b_6, b_7. Pokud je naopak $s_3 = 0$, tak víme, že k chybě nedošlo na žádném z míst, která mají ve dvojkové soustavě 1 na místě stovek, tj. chyba musí být u některé z cifer na místech, která mají cifru 0 na místě stovek, tj. u některé z cifer b_1, b_2, b_3. Chybně přenesená je tedy cifra b_3. Všimněme si, že místo $3 = s_3\, s_2\, s_1 = 011$ při vyjádření ve dvojkové soustavě. Změníme-li cifru b_3, bude nové slovo vyhovovat všem třem rovnicím definujícím Hammingův kód, bude tedy kódovým slovem.

7. PŘÍKLADY UŽITÍ SAMOOPRAVNÝCH KÓDŮ

Teorie kódování se zabývá tím, jak rychle a spolehlivě přenášet informace z jednoho místa na druhé. Mezi její aplikace patří například minimalizace šumu při přehrávání kompaktních disků, přenos finančních informací po telefonních linkách, přenos informací mezi dvěma počítači, mezi pevným diskem a operační pamětí v jednom počítači, přenos informací z telekomunikačních, meteorologických nebo špionážních satelitů, přenos obrázků vzdálených planet a jejich měsíců ze sondy Voyager zpátky na Zem, atd. Fyzikální prostředí, ve kterém je informace přenášena, se nazývá kanál.

Příkladem kanálů mohou být atmosféra, telefonní linky, elektromagnetické pole, atd. Při přenosu informace kanálem může dojít k jejímu poškození kvůli poruchám fyzikálního prostředí, ve kterém k přenosu dochází. Obecně jim říkáme šum. Šum může být způsobený například slunečními skvrnami, bleskem, přehnutím magnetické pásky, přeslechem u telefonních linek, překlepy při psaní, špatnou artikulací, nedoslýchavostí, poškrábáním kompaktního disku, atd.

Šum může způsobit, že přijatá zpráva se liší od zprávy vyslané. Teorie kódování se zabývá problémem jak odhalit a opravit chyby způsobené šumem v komunikačním kanálu. Schematicky můžeme znázornit systém pro přenos informací pomocí obrázku.



Z našeho pohledu je nejdůležitější částí diagramu šum. Bez něho by teorie kódování nebyla třeba. Šum můžeme zmenšit pomocí volby vhodného komunikačního kanálu a použitím filtrů, které dokáží šum minimalizovat. Poté, co jsme už z dostupných možností vybrali vhodný komunikační kanál, můžeme obrátit pozornost na konstrukci kódovacího a dekódovacího zařízení.

Konstrukce kódovacího a dekódovacího zařízení sleduje několik cílů:

1. rychlé kódování informace,
2. snadný přenos zakódované zprávy,
3. rychlé dekódování přijaté zprávy,
4. opravu chyb způsobených šumem v kanálu během přenosu zprávy,
5. maximalizaci množství informace přenesené za jednotku času.

Každý přirozený jazyk má v sobě zabudovánu možnost opravy chyb způsobených šumem, kterým může být v tomto případě sbíječka za oknem, špatná artikulace,

nedoslýchavost, překlepy, apod. Tato ochrana před šumem je tak přirozená, že si ji ani neuvědomujeme. Odolnost přirozeného jazyka vůči šumu je založena na redundanci, nadbytečnosti používaných hlásek pro přenos dané informace. Většině českých vět lze rozumět, i když vynecháme všechny samohlásky: zkuste si sami domyslet, co jsem dělal v sobotu večer: “V sbt včr jsm šl s kmrdm n pv”.
Obvykle se odhaduje, že redundance přirozeného jazyka je více než 50%. To znamená, že stejné množství informace je možné sdělit s méně než polovinou hlásek.

7.1. Cyklický kód

Definice

Cyklický kód je lineární kód dimense k a délky n, pokud $(a_{n-1}, a_{n-2},\ldots, a_1, a_0)$ je kódové slovo, tak také cyklický posun $(a_{n-2},\ldots, a_2, a_1, a_{n-1},)$ je kódové slovo.

Cyklický posun

Vektor $v=(a_{n-1}, a_{n-2},\ldots, a_1, a_0)$ chápeme jako polynom $v(x)=a_{n-1}\cdot x^{n-1}+$ $+a_{n-2}\cdot x^{n-2}+\ldots+a_1\cdot x+a_0$ stupně menšího nebo rovno $n-1$ nad Z_p. Potom $a_{n-2}\cdot x^{n-1}+\ldots+a_1\cdot x^2+a_0\cdot x+a_{n-1}=x\cdot v(x)$ v $Z_p[x]/(x^n-1)$.

Vlastnosti:

- polynomy $v=v_1,\ldots, v_r$ jsou kódovými slovy a spolu s libovolnými prvky $\alpha_1,\ldots,\alpha_r$ v Z_p tvoří lineární kombinaci $\alpha_1 v_1+\ldots+\alpha_r v_r$, která je také kódovým slovem.
- $v(x)$ je kódové slovo, $p(x)$ je libovolný polynom v $Z_p[x]/(x^n-1)$ je součin $p(x)\cdot v(x)$ také kódové slovo.
- obsahuje nenulové slovo, obsahuje slovo $g(x)$ stupně $n-k$, potom kódová slova jsou $p(x)\cdot g(x)$, kde $p(x)$ je polynom stupně menšího než k.

Příklad

cyklického kódu délky $n=4$

$$0000 \approx 0 = 0\cdot(1+x)$$

$$1100 \approx 1+x = 1\cdot(1+x)$$

$$1010 \approx 1+x^2 = (1+x)\cdot(1+x)$$

$$1001 \approx 1+x^3 = (1+x+x^2)\cdot(1+x)$$

$$0110 \approx x+x^2 = x\cdot(1+x)$$

$$0101 \approx x+x^3 = (x+x^2)\cdot(1+x)$$

$$0011 \approx x^2+x^3 = x^2\cdot(1+x)$$

$$1111 \approx 1+x+x^2+x^3 = (1+x^2)\cdot(1+x)(1+x)$$

Nenulový polynom $(1+x)$ je nejnižšího stupně a následující polynomy jsou jeho násobkem.

Nejznámější cyklické kódy jsou BCH kódy, pojmenované podle svých objevitelů. Nejznámějším BCH kódem jsou Reed-Solomonovy kódy. Ty se používají pro ochranu informací, které jsou uloženy na CD a DVD, zabezpečují přenos dat v technologiích DSL a WiMAX a přenos televizního signálu ve formátu DVB a ATSC.

Příklad 7.1

Vytvořte cyklický kód

$f(x)=x^8+x^7+x^4+x+1,\ g(x)=x^4+x^3+1$

Řešení:

$g(x)=x^4+x^3+1 \rightarrow r=4 \rightarrow x^4\cdot f(x)=x^{12}+x^{11}+x^8+x^5+x^4$

$$\left(x^{12}+x^{11}+x^8+x^5+x^4\right):\left(x^4+x^3+1\right)=x^8+x$$

$$\underline{-x^{12}-x^{11}-x^8}$$

$$\underline{\qquad 0 \quad +x^5+x^4}$$

$$\underline{\qquad\qquad -x^5-x^4-x}$$

$$x$$

Zbytkem polynomů je polynom $s(x) = x$.

Zabezpečené kódové slovo: $x^4 \cdot f(x) + s(x) = x^{12} + x^{11} + x^8 + x^5 + x^4 + x$.

7.2. BCH kódy

Tyto kódy jsou nejdůležitější třída cyklických kódu. Jsou označovány podle svých objevitelů Bose-Chaudhuriho-Hocquegha. U těchto kódu je relativně malá délka slova.

Definice

Nechť T je těleso s charakteristikou p. Minimální polynom prvku $a \in T$ je polynom $f(x)$ nad tělesem Z_p minimálního stupně takový, že platí $f(a) = 0$.

Jedná se o cyklické kódy $BCH_{q,m,\delta}$, kde q je velikost abecedy, m určuje délku kódu, která je dána vztahem $n = q^m - 1$ a δ je zadaná vzdálenost kódu.

Parametry těchto kódů zapisuje $[n, k, d]_q$, kde $n = q^m - 1$, $k \geq q^m - m(\delta - 1) - 1$ a $d \geq \delta$.

Prvním řádkem kontrolní matice BCH kódu jsou mocniny generujících kořenů a^i, $i = 0, 1, \ldots, n-1$. Tato čísla představují čtveřice binárních číslic. V druhém řádku je zadán funkcí s argumentem generující kořeny $f(a^i)$.

7.3. Konvoluční kódy

Konvoluční kódy jsou efektivní kódy, které jsou velmi účinné, a proto se velmi často používají v technologiích, jsou vynikající pro opravu jediné bitové chyby a jsou velmi významným prostředkem opravy chyb při satelitním vysílání.

Konvoluční kódy a s kombinací Reed-Solomonovy kódy jsou používány k přenosu signálu na Mars. Tyto signály jsou rušeny během zpátečních cest prostřednictvím vesmíru. Komunikace mezi Zemí a vozítkem není spolehlivá. Kódovací systém používaný v MER závisí právě na dvou různých kódech používaných v kombinaci těchto kódů.

7.4. Reed-Solomonovy kódy

Tyto kódy jsou pojmenovany podle Irvinga S. Reeda a Gustava Solomona a byly představeny v roce 1960.

Tyto kódy jsou třídou BCH kódu. Pro jejich délku slova platí $n = q^m - 1 = q - 1$, kde $m = 1$.

Definice

Generující polynom $g(x)$ je vyjádřen výrazem $(x-\beta)\left(x-\beta^2\right)\cdots\left(x-\beta^{2t}\right)$. $\beta, \beta^2 \ldots \beta^{2t}$ jsou kořenové součinitele, řád n součinitelů β je počtem prvku n zmenšených o jedničku. Minimální kódová vzdálenost je $d_{\min} = 2t + 1$.

Poznámka: Je to vždy polynom stupně $2t$.

Kódy se nejčastěji používají pro zabezpečování diskových magnetických i optických pamětí. Hlavním zdrojem chyb na kompaktních discích jsou nedokonalosti vzniklé při výrobě disku, např. otisky prstu, škrábance, prach, povrchová poškození.

ZÁVĚR

Hlavním cílem této práce bylo vytvoření relativně uceleného přehledu základu teorie jednoho užití polynomů nad konečnými tělesy, které jsme využili při kódovaní a dekódování.

Tato práce je pro větší přehlednost rozdělena do několika kapitol. Ukázali jsme si Kroneckerův algoritmus, který je velmi zdlouhavý, a jeho postup je nepraktický, i když vedl vždy k rozkladu polynomů. Pokud bychom daný polynom nemohli rozložit, pak můžeme při tomto algoritmu konstatovat, že polynom je ireducibilní v $\mathbb{Z}[x]$.

Dalším algoritmem, který jsme si podrobně vysvětlili, se nazývá Berlekampův algoritmus, který lze využít v $Z_p[x]$. K zjištění největších společných dělitelů jsme využili Program *Mathematica* 8.

Algoritmy vždy dovedly rozklad mnohočlenu vypočítat a došli jsme k závěru, že rozklad polynomu existoval.

V některých kapitolách se setkáváme s praktickými ukázkami užití této teorie. Teoretický obsah je vhodně doplněn příklady, které jsou vyhotoveny v programu *Mathematica* 8. Tento vědecko-technický nástroj určený pro modelování a simulace urychluje práci s výpočty.

RESUMÉ

In this thesis, we dealt with one solution of polynomials over the field fields. Kronecker's algorithm, which is very lengthy, and its process is impractical, even though it always leads to the decomposition of polynomials. I we can not decompose a given polynomial, then we can say in this algorithm that the polynomial is irreducible in ℤ[x].

Berlekamp algorithm that can be used in $Z_p[x]$. To find the largest common divisors, we used Mathematica 8. The scientific-technical tool, intended for modeling and simulation, speeds up the work with calculations and thanks to visualization may very well be used for demonstration during the interpretation.

The goal is to create a single use of polynomials over the final fields that we used to encode and decode the messages.

SEZNAM LITERARURY:

[1] D.S. Dummit and R. M. Foote, Abstract algebra, third edition. John Wiley & Sons, Inc.,Hoboken, NJ, 2004.

[2] C. F. Gauss, Untersuchungen ¨Uber H¨ohere Arithmetik, second edition, reprinted, Chelsea publishing company, New York 1981.

[3] K. Ireland and M. Rosen, A classical introduction to modern number theory, second edition, Springer-Verlag, GTM Vol 84 (second edition) 1990.

[4] T. W. Judson, Abstract Algebra: Theory and Applications, PWS-Kent, Boston, 1994.

[5] HOLENDA, Jirí; RYJÁCEK, Zdenek. Lineární algebra II, Úvod do diskrétní matematiky. 2. vyd. Plzen: Západoceská univerzita, 2000. 220s.
ISBN 80-7082-638-X.

[6] BICAN, Ladislav; KEPKA, Tomáš. Komutativní algebra. 1. vyd. Praha: Státní pedagogické nakladatelství, 1982. 175s.

[7] Algebra II. Bican, L: Algebra II. Skriptum MFF UK Praha, SPN Praha, 1982

[8] von zur Gathen, J., Bernard, J.: Modern Computer Algebra. Cambridge University Press, 2003

[9] Lidl, R., Niederreiter, H.: Introduction to finite fields and their applications, Cambridge University Press, revidované vydání, 1997.

[10] Procházka, L. a kol.: Algebra, Academia, Praha, 1990

[11] ČVUT v Praze [online].
Dostupný z WWW: <https://math.feld.cvut.cz/gollova/tik/tik_p3.pdf>.
Dostupný z WWW: <https://math.feld.cvut.cz/gollova/tik/tik_p3.pdf>.

[12] Pedagogocká fakulta ZČU v Plzni [online].
Dostupný z WWW: <https://fpe.zcu.cz/kmt/kmt/projekty/projekt_VS_14/1-1.html>.
Dostupný z WWW: <https://fpe.zcu.cz/kmt/kmt/projekty/projekt_VS_14/1-3.html>.

[13] Pedagogická fakulta Univerzity Karlovy v Praze [online].
Dostupný z WWW:< http://www.karlin.mff.cuni.cz/~barto/student/SkriptaKonTel.pdf >.