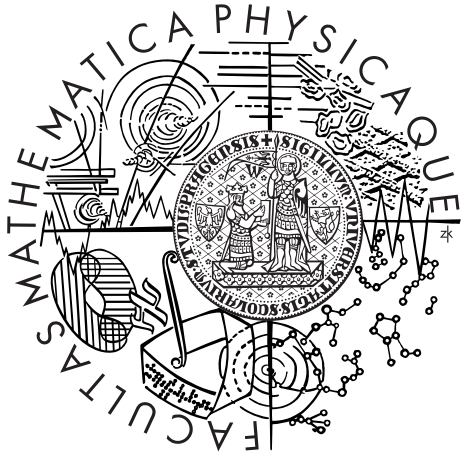
Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

BAKALÁŘSKÁ PRÁCE



David Kubát

Modulární algoritmy a interpolace

Katedra algebry

Vedoucí bakalářské práce:	doc. RNDr. David Stanovský, Ph.D.
Studijní program:	Matematika
Studijní obor:	Matematické metody informační bezpečnosti

Praha 2014

Rád bych poděkoval doc. RNDr. Davidu Stanovskému, PhD. za ochotné vedení této bakalářské práce.

Prohlašuji, že jsem tuto bakalářskou práci vypracoval(a) samostatně a výhradně s použitím citovaných pramenů, literatury a dalších odborných zdrojů.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona v platném znění, zejména skutečnost, že Univerzita Karlova v Praze má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle §60 odst. 1 autorského zákona.

V ..... dne ..... Podpis autora

Název práce: Modulární algoritmy a interpolace

Autor: David Kubát

Katedra: Katedra algebry

Vedoucí bakalářské práce: doc. RNDr. David Stanovský, Ph.D. Katedra algebry

Abstrakt: Tato práce se z algebraického hlediska zabývá problémem polynomiální interpolace a problémem rekonstrukce racionálních funkcí (Cauchyova interpolace, Padého aproximace). Dále zahrnuje některé aplikace zobecněné čínské věty o zbytcích (Hermitova interpolace, rozklady na parciální zlomky). Důležitým teoretickým konceptem pro danou problematiku je Eukleidův algoritmus, kterému je věnována přiměřená pozornost (konkrétně jeho variantě pro obor polynomů). Východiskem je učebnice Modern Computer Algebra od von zur Gathena a Gerharda. Vlastním obsahem práce jsou především řešená cvičení z 5. kapitoly zmíněné učebnice. Ta nejčastěji rozšiřují teorii z učebnice, případně ji doplňují (například důkazy některých tvrzení).

Klíčová slova: interpolace, Eukleidův algoritmus, racionální funkce

Title: Modular algorithms and interpolation

Author: David Kubát

Department: Department of Algebra

Supervisor: doc. RNDr. David Stanovský, Ph.D., Department of Algebra

Abstract: This thesis concerns with the polynomial interpolation problem and the rational function reconstruction problem (Cauchy interpolation, Padé approximation). It does so from the algebraical point of view. Moreover, it involves some applications of the generalized chinese remainder theorem (Hermite interpolation, partial fraction decomposition). An important theoretical concept regarding the above mentioned problems is the Euclidean algorithm, which is studied in case of polynomial rings. The structure of the thesis is based on the book by von zur Gathen and Gerhard called Modern Computer Algebra. Its exercises are the main content of the thesis. They usually extend the theory involved.

Keywords: interpolation, Euclidean algorithm, rational function

Obsah

Úvod

Otázka vhodné reprezentace matematických objektů (čísel, polynomů) je klíčová pro jejich další využití. Kromě obvyklé reprezentace vzhledem k mocninám nějakého základu (např. 2, nebo 10 pro čísla, x pro polynomy) může být výhodná i tzv. modulární reprezentace. Celé číslo takto můžeme reprezentovat pomocí zbytků po jeho dělení různými prvočísly, polynom zase pomocí funkčních hodnot v různých bodech definičního oboru. Vhodnost těchto reprezentací závisí na typu úloh, které s objekty chceme provádět. Například pro násobení polynomů, výpočet determinantů matic, nebo největší společný dělitel celočíselných polynomů existují efektivní algoritmy pracující s modulární reprezentací. Ta však obvykle není pro člověka příliš srozumitelná, je tedy nutné mít k dispozici i algoritmy na převod zpět do reprezentace pomocí mocnin základu. Pro tento účel se v případě celých čísel využívá klasická čínská věta o zbytcích, pro polynomy zase věta o interpolaci.

Obě tyto věty mají společné zobecnění (zobecněná čínská věta o zbytcích, kterou uvádím v první kapitole této práce). Dále se v této bakalářské práci věnuji především problému interpolace. V první kapitole jde o klasickou polynomiální interpolaci a dále Hermitovu interpolaci, ve druhé kapitole se věnuji rozkladům racionálních funkcí na parciální zlomky. Zbytek práce se týká racionálních funkcí: Cauchyova interpolace, Padého aproximace a nakonec racionální čínská věta o zbytcích. Forma, která pro to byla zvolena odpovídá zadání: jde o řešení cvičení z 5. kapitoly učebnice [1]. Výběr úloh byl podmíněn zejména jejich náročností. Mnoho cvičení se do práce nehodilo, jelikož byly buď mechanické, nebo příliš jednoduché. Snažil jsem se naopak vybírat takové, které rozšiřují teorii z učebnice, případně jí doplňují (například jako důkazy jednodušších tvrzení). V řešení těchto cvičení spočívá můj vlastní přínos.

1 Čínská věta o zbytcích, interpolace

V první kapitole nejprve stručně shrneme známou teorii týkající se polynomiální interpolace. Jejím hlavním obsahem pak budou řešená cvičení z [1] a nakonec se budeme věnovat problému Hermitovy interpolace.

1.1 Polynomiální interpolace

Všechny důkazy uvedených tvrzení lze nalézt v [1] nebo [2]. V této kapitole budeme jako R vždy značit obor integrity. Pro r,$s \in R$ budeme jako (r) značit ideál generovaný prvkem r, jako $gcd(r,s)$ zase největší společný dělitel r,s. Čínskou větu o zbytcích využijeme i v dalších kapitolách této práce.

Věta 1.1 (čínská věta o zbytcích)**.** *Buď R obor integrity hlavních ideálů, $r \in \mathbb{N}$, m_0,...,$m_{r-1} \in R$, takové, že $gcd(m_i,m_j) = 1$ pro $0 \leq i < j < r$, a dále označme $m = \prod_{i=0}^{r-1} m_i$. Potom existuje izomorfismus okruhů*

$$R/(m) \cong R/(m_1) \times ... \times R/(m_{r-1}).$$

Předpokládejme, že je na R definováno dělení se zbytkem. Izomorfismus z Čínské věty o zbytcích má potom tvar $r \mapsto (r \bmod m_0,...,r \bmod m_{r-1})$. Pro libovolná v_0,...,$v_r \in R$ lze řešení $f \in R$ soustavy kongruencí

$$f \equiv v_i \pmod{m_i} \text{ pro } 0 \leq i < r$$

nalézt pomocí Lagrangeova algoritmu:

1. pro každé $i = 0,...,r-1$ proveď
   (i) $N_i \leftarrow \frac{m}{m_i}$
   (ii) najdi s_i splňující $s_i N_i \equiv 1 \pmod{m_i}$
   (iii) $c_i \leftarrow v_i s_i \bmod m_i$
2. odpověz $\sum_{i=0}^{r-1} c_i N_i$

Důsledkem věty 1.1 je klasická čínská věta o zbytcích pro celá čísla, stejně jako věta o interpolaci. V případě $R = F[x]$, kde F je těleso, má Lagrangeův algoritmus kvadratickou časovou složitost.

Věta 1.2. *Nechť $R = F[x]$, kde F je těleso, m_0,...,$m_{r-1} \in R$, $m = \prod_{i=0}^{r-1} m_i$. Nechť* deg $m_i \geq 1$ *a $v_i \in R$ ať splňují* deg $v_i <$ deg m_i *pro $0 \leq i < r$. Dále označme $n =$* deg m*. Pak má Lagrangeův algoritmus časovou složitost $O(n^2)$ operací v F.*

1.2 Řešená cvičení

Obsahem této sekce jsou řešení vybraných cvičení z [1]. V závorce je vždy uvedeno jejich číslo v této učebnici. V prvním se věnujeme interpolaci v okruhu $\mathbb{Z}_m$, kde m je součinem dvou různých prvočísel ($\mathbb{Z}_m$ tedy není těleso, ani obor integrity).

Úloha 1.1 (5.22)**.** *Nechť* p_0,$p_1 \in \mathbb{N}$ *jsou různá prvočísla,* $m = p_0p_1$, $n \in \mathbb{N}$ *a* $u_0,...,u_{n-1}, v_0,...,v_{n-1} \in \mathbb{Z}$.

(i) Dokažte, že polynom $f \in \mathbb{Z}[x]$ *takový, že*

$$\text{koeficienty } f \text{ leží v množině } \{0,...,m-1\},\ \deg f < n \text{ a } f(u_i) \equiv v_i \ (mod\ m) \tag{1}$$

pro $0 \le i < n$*, existuje, právě když platí implikace*

$$u_i \equiv u_j \ (mod\ p_k) \implies v_i \equiv v_j \ (mod\ p_k), \tag{2}$$

$0 \le i < j < n$, $k = 0,1$.

(ii) Ukažte, že (1) *má jednoznačné řešení* $\iff$ $u_i \not\equiv u_j \ (mod\ p_k)$ *pro každé* $0 \le i < j < n$, $k = 0,1$.

(iii) Spočtěte všechny interpolační polynomy $f \in \mathbb{Z}[x]$ *s koeficienty z množiny* $\{0,...,14\}$, $\deg f < 3$ *splňující*

$$f(1) \equiv 2 \ (mod\ 15)$$

$$f(2) \equiv 5 \ (mod\ 15)$$

$$f(4) \equiv -1 \ (mod\ 15).$$

Řešení. (i) Hledáme polynom $f \in \mathbb{Z}_m[x]$, $f = \sum_{j=0}^{n-1} c_j x^j$, takový, že $f(\bar{u}_i) = \bar{v}_i$ pro každé $i = 0,...n-1$, kde $\bar{u}_i = u_i \bmod m$, $\bar{v}_i = v_i \bmod m$. Bez újmy na obecnosti můžeme předpokládat, že všechny $u_i, v_i \in \mathbb{Z}_m$. Nechť $\varphi : \mathbb{Z}_m \to \mathbb{Z}_{p_0} \times \mathbb{Z}_{p_1}$ je izomorfismus okruhů z Čínské věty o zbytcích. Pak

$$f(u_i) = v_i \iff \varphi(f(u_i)) = \varphi(v_i) \iff \varphi(\sum_{j=0}^{n-1} c_j u_i^j) = \varphi(v_i)$$

$$\iff \sum_{j=0}^{n-1} \varphi(c_j)\varphi(u_i)^j = (v_i \bmod p_0,\ v_i \bmod p_1)$$

$$\iff \sum_{j=0}^{n-1} (c_j \bmod p_0)(u_i \bmod p_0)^j = v_i \bmod p_0 \text{ a zároveň}$$

$$\sum_{j=0}^{n-1} (c_j \bmod p_1)(u_i \bmod p_1)^j = v_i \bmod p_1$$

pro každé $i \in \{0,...,n-1\}$. Nyní je vidět, že hledaný polynom f existuje, právě když existují polynomy $g_k \in \mathbb{Z}_{p_k}[x]$,

$$\deg g_k < n, \text{ takové, že } g_k(u_i \bmod p_k) = v_i \bmod p_k,\ i = 0,...,n-1, \tag{3}$$

$k = 0,1$. Pokud však existuje trojice $(i,j,k) \in \{0,...,n-1\}^2 \times \{0,1\}$ taková, že $i \neq j$, $u_i \equiv u_j \pmod{p_k}$, $v_i \not\equiv v_j \pmod{p_k}$, pak polynom g_k s požadovanou vlastností existovat nemůže, a neexistuje tedy ani hledaný polynom f. Předpokládejme, že platí (2). Pak každé dvě dvojice $(u_i \bmod p_k, v_i \bmod p_k)$, $(u_j \bmod p_k, v_j \bmod p_k)$

jsou buď stejné, nebo $u_i \not\equiv u_j \pmod{p_k}$. Pro $k \in \{0,1\}$ označme
$d_k := |\{(u_i \bmod p_k, v_i \bmod p_k) : 0 \leq i < n\}|$. Podle věty o interpolaci pak existuje pro každé k polynom $g_k \in \mathbb{Z}_{p_k}[x]$, $\deg g_k < d_k \leq n$ splňující (3). Tím je důkaz hotov.

(ii) Hledaný polynom $f \in \mathbb{Z}_m[x]$ je určen jednoznačně, právě když pro každé $k \in \{0,1\}$ je polynom $g_k \in \mathbb{Z}_{p_k}[x]$ splňující (3) určen jednoznačně. Nechť pro $k \in \{0,1\}$ je $d_k < n$, $g_k \in \mathbb{Z}_{p_k}[x]$ splňuje (3) a $\deg g_k < d_k$. Nechť dále $a_1 := u_1 \bmod p_k, \ldots, a_{d_k} := u_{d_k} \bmod p_k \in \mathbb{Z}_{p_k}$ jsou po dvou různé. Pak polynom $h(x) = g_k(x) + \prod_{i=1}^{d_k}(x - a_i) \in \mathbb{Z}_{p_k}[x]$ splňuje (3) a $g_k \neq h$. Pokud naopak $d_k = n$, pak je podle věty o interpolaci polynom g_k splňující (3) určen jednoznačně. Dále zřejmě $d_k = n$, právě když $u_i \not\equiv u_j \pmod{p_k}$ pro každé $0 \leq i < j < n$. Tím je důkoz hotov.

(iii) Najdeme $g_0 \in \mathbb{Z}_3[x]$, $g_1 \in \mathbb{Z}_5[x]$ splňující (3) (kde $n = 3$, $p_0 = 3$, $p_1 = 5$). Jelikož $d_1 = 3 = n$, je polynom g_1 určen jednoznačně a lze ho spočítat (například pomocí Lagrangeova algoritmu) jako $g_1 = 3x^2 + 4x$. Je však $d_0 = 2 < n$ ($u_0 = 1 \equiv 4 = u_2 \pmod 3$) a polynom g_0 jednoznačně určen není. Všechny polynomy $h(x) \in \mathbb{Z}_3[x]$ splňující (3) (pro $k = 0$) jsou tvaru, $h_i(x) = g_0(x) + i(x+1)(x+2)$, kde $g_0 = 2$ je konstantní polynom a $i \in \mathbb{Z}_3$. Pro $i = 0$ to je polynom $h_0(x) = 2$, pro $i = 1$ polynom $h_1(x) = x^2 + 1$ a $h_2(x) = 2x^2$. Pokud potom jako $a_{i2}, a_{i1}, a_{i0} \in \mathbb{Z}_3$ označíme koeficienty polynomu h_i ($h_i = \sum_{j=0}^{2} a_{ij}x^j$), $b_2 = 3$, $b_1 = 4$, $b_0 = 0$ koeficienty polynomu g_1 a položíme $c_{ij} = \varphi^{-1}(a_{ij}, b_j)$, $i,j = 0,1,2$, budou polynomy $f_0(x) = c_{02}x^2 + c_{01}x + c_{00} = 3x^2 + 9x + 5$, $f_1(x) = c_{12}x^2 + c_{11}x + c_{10} = 13x^2 + 9x + 10$, $f_2(x) = c_{22}x^2 + c_{21}x + c_{20} = 8x^2 + 9x$ právě všechny polynomy splňující podmínky ze zadání.

□

Jak je ukázáno například v [1, str. 102], Lagrangeův interpolační polynom stupně menšího než $n \in \mathbb{N}$ lze (pomocí Lagrangeova algoritmu) spočítat pomocí $7n^2 - 7n$ operací v tělese F. Další možností je využít tzv. Garnerův algoritmus (viz [2]). Jeho asymptotická časová složitost (v případě okruhu polynomů) vychází stejně jako složitost Lagrangeova algoritmu. Jak je ale ukázáno v následující úloze, počet elementárních počet operací v tělese potřebných k výpočtu je menší než v případě Lagrangeovy interpolace.

Úloha 1.2 (5.11). *Předpokládejme, že jsou dány prvky $u_0, \ldots, u_{n-1}, v_0, \ldots, v_{n-1}$ tělesa F, kde $u_0, \ldots, u_{n-1}$ jsou po dvou různé. Nechť $f \in F[x]$ je stupně menšího než n, splňující $f(u_i) = v_i$ pro všechna i. Pokud f vydělíme se zbytkem polynomem $x - u_0$, získáme polynom $g \in F[x]$ stupně* $\deg f - 1$ *takový, že $f = (x - u_0)g + f(u_0) = (x - u_0)g + v_0$. Pro $i \geq 1$ pak platí $g(u_i) = (v_i - v_0)/(u_i - u_0)$ a polynom g spočítáme rekurzivně stejným způsobem.*

(i) Na základě předchozích úvah navrhněte algoritmus pro počítání interpolačního polynomu, dokažte jeho správnost a odhadněte jeho časovou složitost. Řešení je možné najít pomocí méně než $5n^2/2$ operací v F.

(ii) Pomocí tohoto algoritmu najděte polynom $f \in \mathbb{F}_7[x]$ stupně nejvýše 2, splňující $f(0) = 1$, $f(1) = 5$, $f(6) = 2$.

Řešení (i) Úlohu řeší algorimus 1.

Algoritmus 1

Vstup: $u_0,...,u_{n-1} \in F$ po dvou různé, $v_0,...,v_{n-1} \in F$, F těleso, $n \geq 2$.
Výstup: $f \in F[x]$ stupně nejvýše $n-1$ splňující $f(u_i) = v_i$ pro $0 \leq i < n$
$t_{0,0} \leftarrow v_0$, $t_{0,1} \leftarrow v_1$, ..., $t_{0,n-1} \leftarrow v_{n-1}$
for $i \leftarrow 1,...,n-1$ **do**
  for $j \leftarrow i,...,n-1$ **do**
    $t_{i,j} \leftarrow (t_{i-1,j} - t_{i-1,i-1})(u_j - u_{i-1})^{-1}$
  end for
end for
$f_{n-1} \leftarrow t_{n-1,n-1}$
for $i \leftarrow n-2, n-3,...,0$ **do**
  $f_i \leftarrow (x - u_i)f_{i+1} + t_{i,i}$
end for
return f_0

Správnost algoritmu dokážeme indukcí podle n. V případě $n = 1$ je výstupem algoritmu konstantní polynom $f_0 = t_{0,0} = v_0 \in F[x]$, který zřejmě splňuje podmínku $\deg f_0 < n = 1$, $f(u_0) = v_0$. Nechť $n > 1$. Podle indukčního předpokladu spňuje polynom f_1 podmínku $\deg f_1 < n-1$, $f_1(u_i) = t_{1,i}$ pro $1 \leq i < n$ a jelikož $f_0 = (x - u_0)f_1(x) + t_{0,0}$, platí

$$f_0(u_0) = t_{0,0} = v_0,$$

a pro $1 \leq i < n$

$$f_0(u_i) = (u_i - u_0)f_1(u_i) + t_{0,0} = (u_i - u_0)t_{1,i} + v_0$$

$$= (u_i - u_0)\frac{t_{0,i} - t_{0,0}}{u_i - u_0} + v_0 = (v_i - v_0) + v_0 = v_i$$

a $\deg f_0 = \deg (x - u_0) + \deg f_1 < 1 + (n-1) = n$.

Co se týče časové složitosti algoritmu, první cyklus proběhne $n(n-1)/2$-krát a v každém kole se provedou tři operace v tělese F (dvakrát odčítání a jedno dělení), za první cyklus tedy celkem $\frac{3}{2}n^2 - \frac{3}{2}n$ operací. Pro odhad složitosti druhé části algoritmu si všimněme, že pro $j \in \{0,...,n-1\}$ je $\deg f_j \leq n - j - 1$. Pro $0 \leq i \leq n-2$ potom součin polynomů $(x - u_i)f_{i+1}$ vyžaduje nejvýše $n - i - 1$ násobení a $n-i-2$ sčítání v F. Po přičtení konstanty $t_{i,i}$ je to celkem $2(n-i-1)$ operací a celý druhý cyklus tedy vyžaduje provedení $\sum_{i=0}^{n-2} 2(n-i-1) = n^2 - n$ operací. Celková časová složitost algoritmu je tedy

$$\frac{3}{2}n^2 - \frac{3}{2}n + n^2 - n \leq \frac{5}{2}n^2$$

operací v F.

(ii) Položíme $t_{0,0} = v_0 = 1$, $t_{0,1} = v_1 = 5$, $t_{0,2} = v_2 = 2$, dále $u_0 = 0$, $u_1 = 1$, $u_2 = 6$. Podle předpisu z algoritmu 1 spočítáme

$$t_{1,1} = \frac{t_{0,1} - t_{0,0}}{u_1 - u_0} = 4,\ t_{1,2} = \frac{t_{0,2} - t_{0,0}}{u_2 - u_0} = 6,\ t_{2,2} = \frac{t_{1,2} - t_{1,1}}{u_2 - u_1} = 6$$

a

$$f_2 = t_{2,2} = 6,$$

$$f_1 = (x-u_1)f_2 + t_{1,1} = (x+6)6 + 4 = 6x + 5,$$
$$f_0 = (x-u_0)f_1 + t_{0,0} = x(6x+5) + 1 = 6x^2 + 5x + 1$$

a f_0 je hledaný polynom.

□

Další úloha ukazuje, že za jistých podmínek je možné omezit se při interpolaci pouze na sudé (případně liché) polynomy.

Úloha 1.3 (5.12)**.** *Nechť F je těleso, $u_0,...,u_{n-1} \in F \setminus \{0\}$ takové, že $u_i \neq \pm u_j$ pro $0 \leq i < j < n$ a $v_0,...,v_{n-1} \in F$.*

(i) Nechť $f \in F[x]$ je polynom stupně menšího než $2n$, splňující $f(u_i) = f(-u_i)$ pro $0 \leq i < n$. Dokažte, že $f(x) = f(-x)$, a tedy f je sudý.

(ii) Použijte větu o interpolaci a předchozí část cvičení, abyste ukázali, že existuje jednoznačně určený sudý polynom $f \in F[x]$ stupně menšího než $2n$, splňující $f(u_i) = v_i$ pro $0 \leq i < n$.

(iii) Buď $g \in F[x]$ jednoznačně určený polynom stupně nejvýše $n-1$ splňující $g(u_i^2) = v_i$, $i = 0,...,n-1$. Jaký je vztah polynomu f z předchozí části cvičení k polynomu g?

(iv) Uveďte analogické tvrzení jako v (i)-(iii) týkající se lichých polynomů.

Řešení. (i) Polynom $g(x) := f(x) - f(-x)$ je stupeně menšího než $2n$ a zároveň pro každé $i \in \{0,...,n-1\}$ platí $g(u_i) = f(u_i) - f(-u_i) = 0$, $g(-u_i) = f(-u_i) - f(u_i) = 0$. Má tedy $2n$ různých kořenů a je to nutně nulový polynom. Odtud $f(x) = f(-x)$.

(ii) Podle věty o interpolaci existuje polynom $f \in F[x]$, $\deg f < 2n$ takový, že $f(\pm u_i) = v_i$. Podle (i) je takový polynom sudý. Pokud $h \in F[x]$ je sudý polynom takový, že $\deg h < 2n$, $h(u_i) = v_i$, $i = 0,...,n-1$, pak ze sudosti plyne $h(-u_i) = v_i$, $i = 0,...,n-1$ a díky jednoznačnosti interpolačního polynomu máme $h = f$.

(iii) Předně poznamenejme, že díky předpokladu na prvky u_i je splněna podmínka $i \neq j \Rightarrow u_i^2 \neq u_j^2$ a polynom g je korektně definovaný. Dále dokážeme, že pokud $g = \sum_{j=0}^{n-1} c_j x^j$, pak $f = \sum_{j=0}^{n-1} c_j x^{2j}$. Označme $h = \sum_{j=0}^{n-1} c_j x^{2j}$. Vzhledem k podmínce jednoznačnosti z předchozí části cvičení stačí dokázat (zřejmě $\deg h < 2n$, h je sudý), že $h(u_i) = v_i$, $i = 0,...,n-1$. Ovšem $h(u_i) = \sum_{j=0}^{n-1} c_j u_i^{2j} = \sum_{j=0}^{n-1} c_j (u_i^2)^j = g(u_i^2) = v_i$. Platí tedy $h = f$ a důkaz je hotov.

(iv) Příslušná tvrzení lze formulovat následovně:

- Nechť $f \in F[x]$, $\deg f < 2n$, $f(u_i) = -f(-u_i)$, $i = 0,...,n-1$. Pak f je lichý.
- Existuje jednoznačně určený lichý polynom $f \in F[x]$ stupně nejvýše $2n-1$ splňující $f(u_i) = v_i$ pro $i = 0,...,n-1$.
- Nechť $g \in F[x]$, $\deg g < n$, $g(u_i^2) = \dfrac{v_i}{u_i}$ pro $i = 0,...,n-1$. Jestliže $g = \sum_{j=0}^{n-1} c_j x^j$, pak $f = \sum_{j=0}^{n-1} c_j x^{2j+1}$.

□

V následujícím cvičení se budeme věnovat interpolaci polynomů dvou proměnných.

Úloha 1.4 (5.13). *Buď F těleso, $n \in \mathbb{N}$, $u_0,...,u_{n-1} \in F$ po dvou různé, $v_i \in F[x]$ pro $i = 0,...,n-1$.*

(i) Navrhněte algoritmus pro výpočet polynomu $f \in F[x,y]$, kde stupeň f v proměnné y je menší než n a

$$f(x,u_i) = v_i(x),\ i = 0,...,n-1.$$

Ukažte, že f je určen jednoznačně.

(ii) Za předpokladu, že stupeň v_i je menší než $m \in \mathbb{N}$ pro každé i, odvoďte časovou složitost vašeho algoritmu.

(iii) Spočítejte $f \in \mathbb{F}_{11}[x,y]$ takový, že

$$f(x,0) = x^2 + 7,\ f(x,1) = x^3 + 2x + 3,\ f(x,2) = x^3 + 5.$$

Řešení. (i) Předpokládejme, že pro každé $i \in \{0,...,n-1\}$ platí $\deg v_i < m$, $m \in \mathbb{N}$. Dále pro každé i označme $v_i(x) = b_{i,m-1}x^{m-1}+...+b_{i,0}$. Uvažme následující algoritmus.

Algoritmus 2

Vstup: $u_0,...,u_{n-1} \in F$ po dvou různé, $v_0,...,v_{n-1} \in F[x]$
Výstup: $f \in F[x,y]$ takový, že $\deg_y f < n$ a $f(x,u_i) = v_i(x)$, $i = 0,...,n-1$.
for $j \leftarrow 0,...,m-1$ **do**
  Spočítej polynom $c_j \in F[y]$, $\deg c_j < n$, splňující $c_j(u_i) = b_{i,j}$ pro $i = 0,...,n-1$
end for
return $f(x,y) = \sum_{j=0}^{m-1} c_j(y)x^j$

Stupeň f v proměnné y je zřejmě menší než n a pro $i \in \{0,...,n-1\}$ dále platí $f(x,u_i) = c_{m-1}(u_i)x^{m-1} + ... + c_0(u_i) = b_{i,m-1}x^{m-1} + ... + b_{i,0} = v_i(x)$.

Pokud $h(x,y) \in F[x,y]$ má v proměnné y stupeň menší než n a zároveň splňuje $h(x,u_i) = v_i(x)$ pro každé $i \in \{0,...,n-1\}$, můžeme vyjádřit $h(x,y) = h_{m-1}(y)x^{m-1} + ... + h_0(y)$, kde $h_0,...,h_{m-1} \in F[y]$ jsou polynomy stupně menšího než n. Potom $f(x,y) - h(x,y) = (c_{m-1}(y) - h_{m-1}(y))x^{m-1} + ... + (c_0(y) - h_0(y))$ a $f(x,u_i) - g(x,u_i)$ je nulový polynom pro každé i. Pro každé i tedy $c_{m-1}(u_i) - h_{m-1}(u_i) = 0$ a protože stupeň polynomu $c_{m-1}(y) - h_{m-1}(y) \in F[y]$ je menší než n, je to nutně nulový polynom a $c_{m-1} = h_{m-1}$. Podobně odvodíme, že $c_{m-2} = h_{m-2},...,c_0 = h_0$ a polynom f je určen jednoznačně.

(ii) Pro dané $j \in \{0,...,m-1\}$ lze podle věty 1.2 polynom $c_j \in F[y]$, $\deg c_j < n$, splňující $c_j(u_i) = b_{i,j}$, $i = 0,...,n-1$, spočítat pomocí $O(n^2)$ operací v tělese F. Celková časová složitost algoritmu 2 je tedy $mO(n^2) = O(mn^2)$ operací v tělese F.

(iii) Máme

$$u_0 = 0,\ u_1 = 1,\ u_2 = 2,$$
$$v_0(x) = x^2 + 7,\ v_1(x) = x^3 + 2x + 3,\ v_2(x) = x^3 + 5$$

a hledáme polynom $f(x,y) = c_3(y)x^3 + c_2(y)x^2 + c_1(y)x + c_0(y)$, kde

$$\begin{array}{llll} c_3(u_0)=0 & c_2(u_0)=1 & c_1(u_0)=0 & c_0(u_0)=7 \\ c_3(u_1)=1 & c_2(u_1)=0 & c_1(u_1)=2 & c_0(u_1)=3 \\ c_3(u_2)=1 & c_2(u_2)=0 & c_1(u_2)=0 & c_0(u_2)=5 \end{array}$$

Polynomy c_3,c_2,c_1,$c_0 \in F[y]$ lze spočítat jako $c_0(y) = 3y^2+4y+7$, $c_1(y) = 9y^2+4y$, $c_2(y) = 6y^2 + 4y + 1$, $c_3(y) = 5y^2 + 7y$ a výsledkem je tedy

$$f(x,y) = (5y^2 + 7y)x^3 + (6y^2 + 4y + 1)x^2 + (9y^2 + 4y)x + 3y^2 + 4y + 7$$

□

1.3 Hermitova interpolace

Hermitova interpolace je zobecněním klasické Lagrangeovy interpolace. Umožňuje najít polynom takový, že kromě předepsaných funkčních hodnot nabývá i předepsaných hodnot derivací. Nejprve tento problém definujme obecně.

Nechť F je těleso, $u_0,...,u_{r-1} \in F$ po dvou různé, $e_0,...,e_{r-1} \in \mathbb{N}$, $v_0,...,v_{r-1} \in F[x]$ a $\deg v_i < e_i$, $0 \leq i < r$. Problémem **Hermitovy interpolace** rozumíme najít polynom $f \in F[x]$ stupně menšího než $n = e_0 + ... + e_{r-1}$ splňující

$$f \equiv v_i \pmod{(x-u_i)^{e_i}} \tag{4}$$

pro každé $i \in \{0,...,r-1\}$.

Následující tvrzení je důsledkem věty 1.1.

Tvrzení 1.3. *Buďte $u_0,...,u_{r-1} \in F$ po dvou různé, $e_0,...,e_{r-1} \in \mathbb{N}$, $v_0,...,v_{r-1} \in F[x]$ a $\deg v_i < e_i$, $0 \leq i < r$. Potom existuje jednoznačně určený polynom $f \in F[x]$, $\deg f < n$, splňující* (4).

Z věty 1.2 dále plyne:

Důsledek 1.4. *Problém Hermitovy interpolace popsaný výše lze vyřešit pomocí $O(n^2)$ operací v tělese F.*

Nyní se podíváme na to, jak výše popsaný problém Hermitovy interpolace souvisí s derivací polynomu. Nejprve připomeneme známé definice. Jako R opět značíme obor integrity.

Definice 1.5. *Nechť $f = \sum_{i=0}^{n} c_i x^i \in R[x]$. Derivaci polynomu f definujeme jako polynom*

$$f'(x) = \sum_{i=0}^{n-1} (\underbrace{1 + ... + 1}_{(i+1)\times}) a_{i+1} x^i$$

pokud $n \geq 1$ a jako nulový polynom, pokud $\deg f \leq 0$. *Derivace vyšších řádů pak definujeme induktivně*

$$f^{(0)} = f,\ f^{(k+1)} = (f^{(k)})',$$

kde $k \in \mathbb{N}$.

Pokud $R \leq \mathbb{C}$, pak má uvedená definice stejný význam, jako definice derivace ve smyslu matematické analýzy. Pro $l \in \mathbb{N}$ budeme dále $l \in R$ chápat jako $\underbrace{1 + ... + 1}_{l\times} \in R$. Následující tvrzení je dokázáno například v [3].

Tvrzení 1.6. *Nechť f,$g \in R[x]$ a $n \in \mathbb{N}$. Pak*

(i) $(f+g)^{(n)} = f^{(n)} + g^{(n)}$

(ii) $(fg)^{(n)} = \sum_{i=0}^{n} \binom{n}{i} f^{(i)} g^{(n-i)}$

(iii) $(f^n)' = nf^{n-1}f'$

Lemma 1.7. *Nechť $f \in R[x]$, $\deg f \leq n \in \mathbb{N}$. Pak pro každé $u \in R$ existují jednoznačně určené f_0,...,$f_n \in R$, že $f = f_n(x-u)^n + f_{n-1}(x-u)^{n-1} + ... + f_1(x-u) + f_0$.*

Důkaz. Důkaz existence lze provést indukcí: pro $n = 0$ je tvrzení zřejmé, pokud $n > 0$, pak lze vyjádřit $f(x) = q(x)(x-u)+r$, kde $r \in R$. Položíme $f_0 = r$ a $q(x) = f_n(x-u)^{n-1} + ... + f_1$ podle indukčního předpokladu. Pro důkaz jednoznačnosti předpokládejme, že

$$f_n(x-u)^n + ... + f_1(x-u) + f_0 = g_n(x-u)^n + ... + g_1(x-u) + g_0, \quad (5)$$

g_0,...,$g_n \in R$. Pokud $n = 0$, pak $f_0 = g_0$. Nechť $n > 0$. Z binomické věty je vidět, že vedoucí koeficient polynomu na levé straně (5) je f_n, zatímco vedoucí koeficient polynomu na pravé straně je g_n. Musí platit $f_n = g_n$ a (5) je ekvivalentní s

$$f_{n-1}(x-u)^{n-1} + ... + f_1(x-u) + f_0 = g_{n-1}(x-u)^{n-1} + ... + g_1(x-u) + g_0.$$

Podle indukčního předpokladu je $f_{n-1} = g_{n-1}$,...,$f_0 = g_0$. □

Důsledek 1.8. *Nechť $f \in R[x]$, $\deg f \leq n \in \mathbb{N}$, $f(x) = f_n(x-u)^n + f_{n-1}(x-u)^{n-1} + ... + f_1(x-u) + f_0$. Pak pro každé $e \in \mathbb{N}$, $1 \leq e \leq n$, platí $f \equiv f_{e-1}(x-u)^{e-1} + ... + f_1(x-u) + f_0 \pmod{(x-u)^e}$.*

Pozorování 1.9. *Všimněme si, že k-tá derivace polynomu $f(x) = f_n(x-u)^n + f_{n-1}(x-u)^{n-1} + ... + f_1(x-u) + f_0 \in R[x]$, kde $f_i \in R$, $0 \leq k \leq n$, se podle tvrzení 1.6 rovná $f^{(k)}(x) = n(n-1)...(n-k+1)f_n(x-u)^{n-k} + ... + (k!)f_k$. Speciálně tedy $f^{(k)}(u) = (k!)f_k$.*

Lemma 1.10. *Nechť $f \in R[x]$, $\deg f < n = e_0 + ... + e_{r-1}$, $u_i \in R$ po dvou různé, $v_i \in R[x]$, $\deg v_i < e_i$, $i = 0,...,r-1$. Pak*

$$f \equiv v_i \ (mod\ (x-u_i)^{e_i}),\ 0 \leq i < r,$$

právě když

$$f = f_{n-1}(x-u_i)^{n-1} + ... + f_1(x-u_i) + f_0 \Rightarrow f_{e_i-1}(x-u_i)^{e_i-1} + ... + f_0 = v_i(x),\ 0 \leq i < r,$$

kde f_0,...,$f_n \in R$.

Důkaz. Nechť $f \equiv v_i \pmod{(x-u_i)^{e_i}}$, $f = f_{n-1}(x-u_i)^{n-1} + ... + f_1(x-u_i) + f_0$, $0 \leq i < r$. Potom podle důsledku 2.4 $f \equiv f_{e_i-1}(x-u_i)^{e_i-1} + ... + f_1(x-u_i) + f_0 \pmod{(x-u_i)^{e_i}}$. Z tranzitivity relace $\equiv$ plyne $v_i \equiv f_{e_i-1}(x-u_i)^{e_i-1} + ... + f_1(x-u_i) + f_0 \pmod{(x-u_i)^{e_i}}$. Jelikož jsou oba polynomy stupně menšího než e_i, musí se rovnat. Opačná implikace neříká nic jiného, než důsledek 1.8. □

Připomeňme, že pro obor integrity R definujeme charakteristiku R jako nejmenší $n \in \mathbb{N}$ takové, že $\underbrace{1 + ... + 1}_{n\times} = 0$, pokud takové n existuje, jinak je charakteristika R rovná 0. Předpokládejme, že F je těleso nulové charakteristiky. Problém Hermitovy interpolace je potom ekvivalentní nalezení polynomu $f \in F[x]$, jehož prvních e_i derivací (počínaje nultou) v bodě u_i nabývá předepsaných hodnot z F (opět předpokládáme, že u_i jsou po dvou různé prvky tělesa F). Přesněji řečeno, hledáme polynom f stupně menšího než $n = e_0 + ... + e_{r-1}$ splňující

$$f(u_0) = c_{0,0},...,f^{(e_0-1)}(u_0) = c_{0,e_0-1}$$

$$\vdots$$

$$f(u_{r-1}) = c_{r-1,0},...,f^{(e_{r-1}-1)}(u_{r-1}) = c_{r-1,e_{r-1}-1},$$

kde $c_{i,j} \in F$, $0 \leq i < r$, $0 \leq j < e_i$ jsou předepsané hodnoty. Položme potom pro $0 \leq i < r$

$$v_i(x) = \frac{c_{i,e_i-1}}{(e_i-1)!}(x-u_i)^{e_i-1} + ... + c_{i,1}(x-u_i) + c_{i,0}$$

a nechť f je řešení problému Hermitovy interpolace s parametry $u_0,...,u_{r-1},e_0,...,e_{r-1}$, $v_0,...,v_{r-1}$. Pro každé i pak podle lemmatu 1.7 můžeme vyjádřit f jako $f(x) = f_{n-1}(x-u_i)^{n-1} + ... + f_1(x-u_i) + f_0$. Podle pozorování 1.9 platí pro každé $0 \leq k < e_i$

$$f^{(k)}(u_i) = (k!)f_k$$

a podle lemmatu 1.10

$$f_k = \frac{c_{i,k}}{(k!)}.$$

Dostáváme tedy $f^{(k)}(u_i) = c_{i,k}$ pro každé $i \in \{0,...,r-1\}$, $k \in \{0,...,e_i-1\}$.

Úloha 1.5. *Najděme polynom $f \in \mathbb{Q}[x]$ stupně nejvýše 5 splňující*

$$f(0) = 1,\ f'(0) = 0,\ f''(0) = -2$$

$$f(1) = 1,\ f'(1) = 2,\ f''(1) = 10.$$

Řešení. Označme

$$v_0(x) = \frac{(-2)}{(2!)}x^2 + 1 = -x^2 + 1$$

$$v_1(x) = \frac{10}{(2!)}(x-1)^2 + 2(x-1) + 1 = 5x^2 - 8x + 4.$$

Polynom f splňující

$$f \equiv v_0(x) \pmod{x^3},$$
$$f \equiv v_1(x) \pmod{(x-1)^3},$$

najdeme například pomocí Lagrangeova algoritmu jako

$$f(x) = x^4 - x^2 + 1$$

a derivováním lze ověřit, že takový polynom splňuje podmínky ze zadání.

□

2 Rozklady na parciální zlomky

V této části ukážeme efektivní algoritmus pro rozklad racionální funkce na parciální zlomky. Potřeba řešit takový problém nastává například při integrování racionálních funkcí. Nejprve definujeme pojem p-adického rozkladu a ukážeme algoritmus na jeho výpočet.

2.1 p-adická reprezentace polynomů

Definice 2.1. *Buď R okruh, a,$p \in R[x]$, kde p je monický stupně $m > 0$ a a je stupně menšího než km, pro k,$m \in \mathbb{N}$. p-adický rozvoj polynomu a je výraz*

$$a = a_{k-1}p^{k-1} + ... + a_1 p + a_0,$$

kde a_0,...,$a_{k-1} \in R[x]$ jsou stupně menšího než m.

p-adický rozvoj polynomu lze počítat podle algoritmu 3.

Algoritmus 3 p-adický rozvoj

Vstup: $p \in R[x]$ monický stupně $m > 0$, $k \in \mathbb{N}$, $a \in R[x]$ je stupně menšího než km
Výstup: a_0,...,$a_{k-1} \in R$ tak, že $a = a_{k-1}p^{k-1} + ... + a_1 p + a_0$
if deg $a < m$ **then**
  return $a_0 = a$ je p-adický rozvoj a
else
  spočti q,$r \in R[x]$ tak, že $a = qp + r$, deg $r < m$
  polož $a_0 = r$
  spočti a_1,...,a_{k-1} tak, že $q = a_{k-1}p^{k-2} + ... + a_2 p + a_1$
  return $a = a_{k-1}p^{k-1} + ... + a_1 p + a_0$ je p-adický rozvoj a
end if

2.2 Rozklad na parciální zlomky

Buď nyní F těleso, f_1,...,$f_r \in F[x]$ jsou nekonstantní, monické a po dvou nesoudělné. Dále nechť e_1,...,$e_r \in \mathbb{N}$ a označme $f = f_1^{e_1}...f_r^{e_r}$. Předpokládejme, že $g \in F[x]$ je stupně menšího než $n = \deg f$. Rozkladem funkce $g/f \in F(x)$ na parciální zlomky vzhledem k dané faktorizaci jmenovatele $f = f_1^{e_1}...f_r^{e_r}$ rozumíme výraz tvaru

$$\frac{g}{f} = \frac{g_{1,1}}{f_1} + ... + \frac{g_{1,e_1}}{f_1^{e_1}} + \ ... \ + \frac{g_{r,1}}{f_r} + ... + \frac{g_{r,e_r}}{f_r^{e_r}}, \tag{6}$$

kde $g_{i,j} \in F[x]$ jsou stupně menšího než f_i pro všechna i,j.

Příklad 2.1. *Pro $F = \mathbb{Q}$, $g(x) = x^3 + x^2 - 2x - 2$, $f(x) = x^4 - x^3 - 2x^2$ bude mít rozklad funkce $g/f \in \mathbb{Q}(x)$ na parciální zlomky vzhledem k faktorizaci $f(x) = x^2(x^2 - x - 2)$ tvar*

$$\frac{x^3 + x^2 - 2x - 2}{x^4 - x^3 - 2x^2} = \frac{1/2}{x} + \frac{1}{x^2} + \frac{x/2 + 1/2}{x^2 - x - 2}$$

□

Jak je dokázáno například v [1], rozklad (6) existuje vždy a navíc je určen jednoznačně. Přirozeným způsobem, jak takový rozklad hledat, je vyjádřit každý polynom $g_{i,j}$ stupně nejvýše deg f_i pomocí neznámých koeficientů a z (6) po přenásobení společným jmenovatelem odvodit soustavu lineárních rovnic s koeficienty polynomů $g_{i,j}$ jako neznámými. Matice takové soustavy má potom rozměr $n \times n$ a pomocí Gaussovy eliminace by její řešení mělo asymptotickou složitost $O(n^3)$. Uvidíme, že postup navržený v [1] je efektivnější.

2.3 Algoritmus na počítání parciálních zlomků

Prvním krokem k rozkladu racionální funkce na parciální zlomky je nalézt $c_i \in F[x]$, deg $c_i <$ $e_i$deg f_i, pro které platí

$$\frac{g}{f} = \frac{c_1}{{f_1}^{e_1}} + ... + \frac{c_r}{f_r^{e_r}} \tag{7}$$

K tomu použijeme algoritmus 4:

Algoritmus 4

Vstup: $f = f_1...f_r \in F[x]$, $g \in F[x]$, kde $f_1,...,f_r \in F[x]$ jsou nekonstantní, monické a po dvou nesoudělné, deg $g <$ deg f.
Výstup: $c_i \in F[x]$, deg $c_i <$ $e_i$deg f_i, splňující (7)
for $i \leftarrow 1,...,r$ **do**
  $N_i \leftarrow f f_i^{-e_i}$
  najdi s_i splňující $s_i N_i \equiv 1 \pmod{f_i^{e_i}}$
  $c_i \leftarrow g s_i \bmod f_i^{e_i}$
end for
return $c_1,...,c_r$

Lze nahlédnout, že pro $c_1,...,c_r$ spočítané podle algoritmu 4 platí následující rovnost:

$$c_i \equiv g \prod_{j \neq i} f_j^{-e_j} \pmod{f_i^{e_i}}$$

pro každé i. Pokud pravou stranu (7) vynásobíme f, získáme polynom $g^* = c_1 f f^{-e_1} + ... + c_r f f^{-e_r}$ jehož stupeň je menší než stupeň polynomu f a pro který platí $g^* \equiv g \pmod{f_i^{e_i}}$ pro každé i. Podle čínské věty o zbytcích je $g^* \equiv g \pmod{f}$ a jelikož jsou oba polynomy stupně menšího než deg f, musí se rovnat. Odtud již plyne vztah (7).

V dalším kroku využijeme algoritmus 3: pokud každé c_i vyjádříme v f_i-adickém rozvoji:

$$c_i = g_{i,1} f_i^{e_i - 1} + ... + g_{i,e_i - 1} f_i + g_{i,e_i},$$

kde $g_{i,j}$ jsou stupně menšího než f_i, budou polynomy $g_{i,j}$ zřejmě splňovat (6). Provedené úvahy doplní následující věta, jejíž důkaz je v [1].

Věta 2.2. *Buď F těleso, $e_1,...,e_r \in \mathbb{N}$, $f_1,...,f_r \in F[x]$ nekonstantní, monické a po dvou nesoudělné, $f = f_1^{e_1}...f_r^{e_r}$, $g \in F[x]$ je stupně menšího než $n =$ deg f. Rozklad na parciální zlomky* (6) *je určen jednoznačně a lze ho spočítat pomocí $O(n^2)$ operací v tělese F.*

Celý postup hledání rozkladů na parciální zlomky nyní ilustrujeme na příkladu z [1].

Úloha 2.1 (5.45)**.** *Rozložte na parciální zlomky funkci*

$$\frac{x+2}{(x+1)^3(x-1)^2} \in \mathbb{Q}(x)$$

Řešení. Označme

$$g(x) = x + 2,$$
$$f_1(x) = x + 1,\ f_2(x) = x - 1.$$

Nyní spočítáme c_1,$c_2 \in \mathbb{Q}[x]$ podle algoritmu 2:

$$N_1(x) = f_2(x)^2 = (x-1)^2,$$

$$\text{pro } s_1(x) = 3/16x^2 + 5/8x + 11/16 \text{ platí } s_1N_1 \equiv 1 \pmod{f_1^3} \text{ a}$$
$$c_1(x) \equiv gs_1 \equiv \frac{1}{16}(7x^2 + 22x + 19) \pmod{f_1^3}.$$

Podobně spočítáme polynom c_2 jako

$$c_2(x) = \frac{1}{16}(-7x + 13).$$

Nyní víme, že

$$\frac{x+2}{(x+1)^3(x-1)^2} = \frac{7x^2+22x+19}{16(x+1)^3} + \frac{-7x+13}{16(x-1)^2}.$$

Dále c_1 vyjádříme v f_1-adickém rozvoji. Jelikož

$$7x^2+22x+19 = (7x+15)(x+1)+4 = (7(x+1)+8)(x+1)+4 = 7(x+1)^2+8(x+1)+4,$$

můžeme c_1 napsat jako

$$c_1(x) = \frac{7}{16}(x+1)^2 + \frac{1}{2}(x+1) + \frac{1}{4}.$$

Podobně

$$c_2(x) = -\frac{7}{16}x + \frac{13}{16} = -\frac{7}{16}(x-1) + \frac{3}{8}.$$

Odtud je již vidět, že

$$\frac{x+2}{(x+1)^3(x-1)^2} = \frac{7}{16(x+1)} + \frac{1}{2(x+1)^2} + \frac{1}{4(x+1)^3} - \frac{7}{16(x-1)} + \frac{3}{8(x-1)^2}.$$

je rozklad dané funkce na parciální zlomky.

□

3 Rekonstrukce racionálních funkcí

3.1 Eukleidův algoritmus

V první části této kaptioly bude nutné připomenout Eukleidův algoritmus a ukázat některé jeho aspekty nad rámec základního kurzu algebry. Začněme s pojmen největšího společného dělitele.

Nechť R je obor integrity. Největší společný dělitel prvků $a,b \in R$ je určen až na asociovanost. Pro každou dvojici $(a,b) \in R^2$ vybereme jednoho reprezentanta z množiny $D(a,b) = \{d \in R : d \mid a,\ d \mid b,\ (c \mid a,\ c \mid b \Rightarrow c \mid d)\}$ a toho budeme značit jako $gcd(a,b)$. V případě $R = F[x]$, F těleso, jsou dva polynomy asociované, právě když se liší o nenulový konstantní násobek. Jako $gcd(a,b)$ pak budeme značit monický polynom z $D(a,b)$.

Algoritmus 5 Rozšířený Eukleidův algoritmus

Vstup: $f,g \in R$, kde R je Eukleidovský obor
Výstup: $l \in \mathbb{N}, r_i,s_i,t_i \in R$ pro $0 \leq i \leq l+1$ takové, že $r_l = s_l f + t_l g \mid\mid gcd(f,g)$
$r_0 \leftarrow f$, $s_0 \leftarrow 1$, $t_0 \leftarrow 0$,
$r_1 \leftarrow g$, $s_1 \leftarrow 0$, $t_1 \leftarrow 1$
$i \leftarrow 1$
while $r_i \neq 0$ **do**
  $q_i \leftarrow r_{i-1}$ div r_i
  $r_{i+1} \leftarrow r_{i-1} - q_i r_i$
  $s_{i+1} \leftarrow s_{i-1} - q_i s_i$
  $t_{i+1} \leftarrow t_{i-1} - q_i t_i$
  $i \leftarrow i + 1$
end while
$l \leftarrow i - 1$
return l,r_i,s_i,t_i pro $0 \leq i \leq l+1$

Jelikož posloupnost norem $\nu(r_1),\nu(r_2),...$ je ostře klesající, musí algoritmus skončit po konečném počtu kroků. Dále ze vztahu $r_{i+1} = r_{i-1} - q_i r_i$ plyne, že dvojice (r_{i-1},r_i) a (r_i,r_{i+1}) mají pro $1 \leq i \leq l$ stejné společné dělitele, a tedy

$$r_l \mid\mid gcd(0,r_l) \;=\; gcd(r_{l+1},r_l) \mid\mid gcd(r_0,r_1) \;=\; gcd(f,g).$$

Další vlastnosti algoritmu 5, na které se dále budeme odvolávat, shrnuje lemma 3.1.

Lemma 3.1. *Pro každé $i \in \{0,...,l\}$ platí*

(i) $r_i = s_i f + t_i g$

(ii) $s_i t_{i+1} - s_{i+1} t_i = (-1)^i$ *a s_i,t_i jsou tedy nesoudělné.*

(iii) $gcd(r_i,t_i) \mid\mid gcd(f,t_i)$

Důkaz. (i) Tvrzení zřejmě platí pro $i = 0$. Nechť $i \geq 0$. Pak podle indukčního předpokladu $r_{i+1} = r_{i-1} - q_i r_i = (s_{i-1} f + t_{i-1} g) - q_i(s_i f + t_i g) = (s_{i-1} - q_i s_i) f + (t_{i-1} - q_i t_i) g$
$= s_{i+1} f + t_{i+1} g.$

(ii) Pro $i = 0$ je tvrzení očividné. Pro $i > 0$ pak můžeme s využitím indukčního předpokladu vyjádřit $s_i t_{i+1} - s_{i+1} t_i = s_i(t_{i-1} - q_i t_i) - (s_{i-1} - q_i s_i)t_i = (-1)(s_{i-1} t_i - s_i t_{i-1}) = (-1)(-1)^{i-1} = (-1)^i$.

(iii) Nechť $d \in R$ dělí t_i. Ukážeme, že $d \mid r_i \iff d \mid f$. Implikace ($\Leftarrow$) plyne okamžitě z (i). Pokud naopak d dělí r_i, pak, opět podle (i), d dělí $s_i f$. Protože s_i,t_i jsou podle (ii) nesoudělné a $d \mid t_i$, jsou d a s_i také nesoudělné. Musí tedy platit $d \mid f$. □

Důkaz následujícího lemmatu je obsahem části cvičení 3.21 z [1].

Lemma 3.2. *Nechť F je těleso, $R = F[x]$. Pak pro každé $i \in \{1,...,l+1\}$ platí*

$$\deg t_i = \deg f - \deg r_{i-1}.$$

Důkaz. Budeme dokazovat

$$\deg t_i = \sum_{1 \le j < i} \deg q_j \tag{8}$$

pro $1 \le i \le l+1$, přičemž

$$\deg q_j = \deg(r_{j-1} \operatorname{div} r_j) = \deg r_{j-1} - \deg r_j$$

a tedy

$$\sum_{1 \le j < i} \deg q_j = \deg f - \deg r_{i-1}$$

(pokud $i = 1$, pak jde o sumu přes prázdnou množinu, která se definitoricky rovná nule, stejně jako rozdíl $\deg f - \deg r_0$). Dále si všimněme, že pro $j \ge 2$ je $\deg q_j = \deg r_{j-1} - \deg r_j > 0$. Indukcí dokážeme, že pro $1 \le i \le l+1$ platí zároveň (8) a $\deg t_{i-1} \le \deg t_i$. Pro $i = 1$ máme $\deg t_1 = \deg 1 = 0 = \sum_{1 \le j < i} \deg q_j$ (opět jde o součet přes prázdnou množinu) a $\deg t_0 = \deg 0 = -1 \le 0 = \deg t_1$ (stupeň nulového polynomu definujeme jako -1). Nechť $1 \le i$ a předpokládejme, že dokazované platí pro $1 \le j \le i$. Nejprve ukážeme, že $\deg(t_{i-1} - q_i t_i) = \deg(q_i t_i)$. Pro $i = 1$, jde o zřejmé pozorování, jelikož $t_{i-1} = t_0 = 0$. Pro $2 \le i$ je podle indukčního předpokladu $\deg t_{i-1} \le \deg t_i < \deg t_i + \deg q_i = \deg q_i t_i$. Nyní je vidět, že $\deg t_{i+1} = \deg(t_{i-1} - q_i t_i) = \deg(q_i t_i) = \deg q_i + \deg t_i \ge \deg t_i$ a zároveň
$\deg t_{i+1} = \deg q_i + \deg t_i = \deg q_i + \sum_{1 \le j < i} \deg q_j = \sum_{1 \le j < i+1} \deg q_j$. □

Pro $j \in \{0,...,l+1\}$ budeme trojici (r_j, s_j, t_j) nazývat j-tý řádek rozšířeného Eukleidova algoritmu. Lemma 3.3 budeme potřebovat v další části. Jeho důkaz lze nalézt v [1].

Lemma 3.3. *Nechť F je těleso, $R = F[x]$ a $f,g,r,s,t \in R$ tak, že $r = sf + tg$, přičemž $t \ne 0$ a $\deg r + \deg t < \deg f$. Nechť dále $r_i, s_i, t_i \in R$, $0 \le i \le l+1$, jsou řádky rozšířeného Eukleidova algoritmu pro vstup f, g a definujme $j \in \{1,...,l+1\}$ tak, že $\deg r_j \le \deg r < \deg r_{j-1}$. Pak existuje $\alpha \in R \setminus \{0\}$ tak, že $r = \alpha r_j$, $s = \alpha s_j$, $t = \alpha t_j$.*

3.2 Rekonstrukce racionálních funkcí obecně

Předpokládejme, že $m \in F[x]$ je stupně $n > 0$, $g \in F[x]$ je stupně menšího než n, $k \in \{0,...,n\}$. Dvojici (r,t) polynomů z $F[x]$ budeme nazývat **$(k,n-k)$-racionalizace** polynomu g modulo m, pokud

- $gcd(t,m) = 1$, $rt^{-1} \equiv g \pmod{m}$
- $\deg r < k$, $\deg t \leq n - k$

případně **slabá $(k,n-k)$-racionalizace** polynomu g modulo m, pokud

- $r \equiv gt \pmod{m}$
- $\deg r < k$, $\deg t \leq n - k$

kde t^{-1} je inverzní prvek k t modulo m. Dále uvidíme, že $(k,n-k)$ racionalizace nemusí existovat pro každé k, slabá $(k,n-k)$ racionalizace polynomu g modulo m však existuje vždy. Uveďme jednoduchý příklad.

Příklad 3.1. *Pokud bude $m = x^2 - 1$, $g = x + 1 \in \mathbb{Q}[x]$, pak $r = 0$, $t = x - 1$ není $(0,2)$-racionalizace polynomu g modulo m, protože $gcd(t,m) = gcd(x-1,x^2-1) = x - 1$, ale je to slabá $(0,2)$-racionalizace polynomu g modulo m.*

O racionální funkci $r/t \in F(x)$ řekneme, že je v kanonickém tvaru, pokud $gcd(r,t) = 1$ a $t \in F[x]$ je monický. Následující věta zajišťuje teoretický podklad pro celý zbytek kapitoly. Její důkaz v [1] využívá lemma 3.3, nicméně postrádá ověření některých jeho předpokladů, proto ho zde uvádím celý.

Věta 3.4. *Nechť $m \in F[x]$ je stupně $n > 0$, $g \in F[x]$ je stupně menšího než n, $k \in \{0,...,n\}$. Nechť dále $r,s,t \in F[x]$ je $j-$tý řádek rozšířeného Eukleidova algoritmu pro vstup m,g, kde j je nejmenší takové, že* $\deg r < k$. *Potom*

(i) Dvojice (r,t) je slabá $(k,n-k)$-racionalizace polynomu g modulo m. Pokud navíc platí $gcd(r,t) = 1$, pak (r,t) je $(k,n-k)$-racionalizace g modulo m.

(ii) Pokud $\frac{\bar{r}}{\bar{t}} \in F(x)$ je v kanonickém tvaru a $(\bar{r},\bar{t})$ je $(k,n-k)$-racionalizace polynomu g modulo m, pak $\bar{r} = \tau^{-1}r$, $\bar{t} = \tau^{-1}t$, kde $\tau = \mathrm{lc}(t) \in F \setminus \{0\}$. Speciálně tedy $(k,n-k)$-racionalizace g modulo m existuje, právě když $gcd(r,t) = 1$.

Důkaz. (i) Podle lemmatu 3.1-(i) platí $r = ms + gt \equiv gt \pmod{m}$. Podle lemmatu 3.2 $\deg t = \deg m - \deg r = n - \deg r$ a tedy $\deg t \leq n - k$ díky minimalitě j. (r,t) je tedy slabá $(k,n-k)$-racionalizace g modulo m. Dále díky lemmatu 3.1-(iii) platí $gcd(r,t) = 1 \Rightarrow gcd(m,t) = 1$, t je v takovém případě invertibilní modulo m a (r,t) je $(k,n-k)$ racionalizace g modulo m.

(ii) Jelikož $\bar{r} \equiv g\bar{t} \pmod{m}$, existuje $\bar{s} \in F[x]$ tak, že $\bar{r} = m\bar{s} + g\bar{t}$. Buď $r_i,s_i,t_i \in F[x]$ $i-$tý řádek rozšířeného Eukleidova algoritmu pro vstup m, g tak, že $\deg r_i \leq \deg \bar{r} < \deg r_{i-1}$ (r_{i-1} je první člen řádku, předcházejícího i-tý). Ukážeme, že $i = j$. Protože $\deg r_i \leq \deg \bar{r} < k$ a j je nejmenší takové, že $\deg r_j < k$, platí $i \geq j$. Dále víme, že $\deg \bar{r} < k$, $\deg \bar{t} \leq n - k$ a je tedy splněn předpoklad $\deg \bar{r} + \deg \bar{t} < n$ lemmatu 3.3 (předpoklad $\bar{t} \neq 0$ také zřejmě platí)

a existuje tedy nenulové $\alpha \in F[x]$ tak, že $\bar{r} = \alpha r_i$, $\bar{s} = \alpha s_i$, $\bar{t} = \alpha t_i$. Nyní ověříme nerovnost $k \leq \deg r_{i-1}$. Platí $\deg \bar{t} = \deg \alpha + \deg t_i \leq n - k$ a podle lemmatu 3.2 $\deg t_i = n - \deg r_{i-1}$, dohromady tedy $\deg \alpha + k \leq \deg r_{i-1}$. Víme, že $\alpha \neq 0$ a tím pádem $k \leq \deg r_{i-1}$. i je tedy nejmenší takové, že $\deg r_i < k$ a nutně $i = j$. Jelikož $\bar{r}$,$\bar{t}$ jsou nesoudělné a α je jejich společný dělitel, musí být α invertibilní, což znamená $\alpha \in F \setminus \{0\}$. Navíc $\bar{t}$ je monický, takže $\alpha = \mathrm{lc}(t_j)^{-1}$. □

3.3 Cauchyova interpolace

Na problém Cauchyovy interpolace lze nahlížet jako na zobecnění problému polynomiální interpolace. Opět budeme mít předepsané funkční hodnoty v různých bodech definičního oboru a cílem bude najít racionální funkci, která v daných bodech nabývá předepsaných hodnot. Podobně jako v případě polynomiální interpolace budeme na takovou funkci klást jisté podmínky týkající se stupňů a uvidíme, že, narozdíl od polynomiální interpolace, nebude taková funkce existovat vždy.

Buď F těleso, $n \in \mathbb{N}$, $k \in \{0,...,n\}$, $u_0,...,u_{n-1} \in F$ po dvou různé, $v_0,...,v_{n-1} \in F$ libovolné. Označme $M = \{(u_0,v_0),...,(u_{n-1},v_{n-1})\} \subseteq F^2$. Dvojici (r,t) polynomů z $F[x]$ nazveme **$(k,n-k)$-Cauchyův interpolant** pro M, pokud

- $t(u_i) \neq 0$ a $\dfrac{r(u_i)}{t(u_i)} = v_i$ pro $0 \leq i < n$
- $\deg r < k$, $\deg t \leq n - k$

V případě, že $k = n$, pak nejde o nic jiného, než o polynomiální interpolaci: zvolíme $t = 1$ a hledáme polynom r stupně menšího než n splňující $r(u_i) = v_i$ pro všechna i. Dále řekneme, že (r,t) je **slabý $(k,n-k)$-Cauchyův interpolant** pro M, pokud

- $r(u_i) = t(u_i)v_i$ pro $0 \leq i < n$
- $\deg r < k$, $\deg t \leq n - k$

Buď nyní $g \in F[x]$ interpolační polynom splňující $g(u_i) = v_i$, $\deg g < n$. Pro každé i pak platí, že $r(u_i) = v_i t(u_i) = g(u_i)t(u_i)$, právě když $r \equiv gt \pmod{(x - u_i)}$. Pokud označíme $m = \prod_{i=0}^{n-1}(x - u_i)$, je podle čínské věty o zbytcích (r,t) slabý $(k,n-k)$-Cauchyův interpolant pro M, právě když je to slabá $(k,n-k)$ racionalizace polynomu g modulo m. Dále je zřejmé, že $t(u_i) \neq 0 \ \forall i \iff gcd(t,m) = 1$. Jinými slovy, (r,t) je $(k,n-k)$-Cauchyův interpolant pro M, právě když je to $(k,n-k)$-racionalizace g modulo m. Díky těmto úvahám a větě 3.4 můžeme nyní zodpovědět otázku existence a jednoznačnosti Cauchyových interpolantů.

Důsledek 3.5. *Buď F těleso, $n \in \mathbb{N}$, $k \in \{0,...,n\}$, $u_0,...,u_{n-1} \in F$ po dvou různé, $v_0,...,v_{n-1} \in F$ libovolné. Označme $M = \{(u_0,v_0),...,(u_{n-1},v_{n-1})\} \subseteq F^2$, $m = \prod_{i=0}^{n-1}(x-u_i)$. Dále buď $g \in F[x]$ stupně menšího než n takový, že $g(u_i) = v_i$ pro všechna i. Nechť $r,s,t \in F[x]$ je j-tý řádek rozšířeného Eukleidova algoritmu pro dvojici m,g, kde j je nejmenší takové, že* $\deg r < k$. *Potom*

(i) (r,t) je slabý $(k,n-k)$-Cauchyův interpolant pro M. Pokud navíc platí $gcd(r,t) = 1$, pak (r,t) je $(k,n-k)$-Cauchyův interpolant pro M.

(ii) Pokud $\frac{\bar{r}}{\bar{t}} \in F(x)$ *je v kanonickém tvaru taková, že* $(\bar{r},\bar{t})$ *je* $(k,n-k)$*-Cauchyův interpolant pro* M*, pak* $\bar{r} = \tau^{-1}r$*,* $\bar{t} = \tau^{-1}t$*, kde* $\tau = \mathrm{lc}(t) \in F \setminus \{0\}$*. Speciálně tedy* $(k,n-k)$*-Cauchyův interpolant existuje, právě když* $gcd(r,t) = 1$*.*

Uvedenou větu ilustrujeme na jednoduchém příkladu.

Úloha 3.1 (5.37)**.** *Pro* $1 \leq k \leq 5$ *zjistěte, zda existují* $(k,5-k)$*-Cayuchovy interpolanty pro* $M = \{(u_0,v_0),...,(u_4,v_4)\} \in \mathbb{F}_5 \times \mathbb{F}_5$*, kde* $u_i = i$*,* $0 \leq i \leq 4$*,* $v_0 = 1$*,* $v_1 = 2$*,* $v_2 = 3$*,* $v_3 = 2$*,* $v_4 = 1$*.*

Řešení. Interpolační polynom $g(x) \in \mathbb{F}_5[x]$ takový, že $g(i) = v_i$, lze obvyklým způsobem spočítat jako $g(x) = x^4 + 2x^3 + 2x^2 + x + 1$, dále $m(x) = \prod_{i=0}^{4}(x-i) = x^5 + 4x$ a rozšířený Eukleidův algoritmus pro dvojici m,g proběhne následovně:

i	r_i	s_i	t_i
0	m	1	0
1	g	0	1
2	$2x^3 + 3x^2 + 2$	1	$4x + 2$
3	3	$2x + 1$	$3x^2 + 3x + 3$
4	0	$2x^4 + 4x^3 + 4x^2 + 2x + 2$	$3x^5 + 2x$

Případ $k = 5$ lze vyřešit volbou $r(x) = g(x) = x^4 + 2x^3 + 2x^2 + x + 1$, $t(x) = 1$. Zajímavější je případ $k = 4$, kdy $j = 2$ je nejmenší j takové, že $\deg r_j < 4$. Jelikož $gcd(r_2,t_2) = gcd(2x^3 + 3x^2 + 2,\ 4x + 2) = x - 2$ je netriviální, je podle lemmatu 3.1 $gcd(m,t_2) = gcd(r_2,t_2) = x - 2$ a $t_2(2) = 0$, takže (r_2,t_2) není (4,1)-Cauchyův interpolant pro M. Podle předchozí věty dokonce žádný (4,1)-Cauchyův interpolant pro M neexistuje. Pro $k = 1,2,3$ bude $j = 3$ a jelikož $gcd(r_3,t_3) = gcd(3,\ 3x^2+3x+3) = 1$, je $(r_3,t_3) = (3,\ 3x^2+3x+3)$ pro $k \in \{1,2,3\}$ $(k,5-k)$-Cauchyův interpolant pro M. Po převodu do kanonického tvaru bude $r = 1$, $t = x^2 + x + 1$ a lze ověřit, že pro každé $i \in \mathbb{F}_5$ platí

$$t(i) \neq 0 \text{ a } \frac{r(i)}{t(i)} = \frac{1}{i^2 + i + 1} = v_i.$$

□

Následující příklad ukazuje jistou nutnou podmínku pro existenci Cauchyových interpolantů.

Úloha 3.2 (5.38)**.** *Buď* F *těleso,* $u_0,...,u_{n-1} \in F$ *po dvou různé,* $v_0,...,v_{n-1} \in F$ *libovolné,* $M = \{(u_0,v_0),...,(u_{n-1},v_{n-1})\}$*,* $k \in \{0,...,n\}$*. Dále označme* $S = \{0 \leq i < n : v_i = 0\}$*. Ukažte, že* $(k,n-k)$*-Cauchyův interpoland neexistuje, pokud* $k \leq |S| < n$*.*

Řešení. Předpokládejme, že (r,t) je $(k,n-k)$-Cauchyův interpolant a $k \leq |S|$. Ukážeme, že $|S| = n$. Protože $\frac{r}{t}(u_i) = 0$ implikuje $r(u_i) = 0$, je r buď nulový, nebo má stupeň aspoň $|S|$. Předpoklad $\deg r < k$ však druhou variantu vylučuje, tudíž je $r = 0$ a $v_i = 0$ pro každé i.

□

3.4 Padého aproximace

Úlohu aproximace funkce v daném bodě pomocí polynomu řeší Taylorův polynom. V případě, že místo polynomu použijeme racionální funkci, půjde o tzv. Padého aproximaci.

Nechť F je těleso, $n \in \mathbb{N}$, $k \in \{0,...,n\}$ a $g = \sum_{i \geq 0} g_i x^i \in F[[x]]$, kde $F[[x]]$ je okruh formálních mocninných řad. Potom racionální funkce $r/t \in F(x)$, $r,t \in F[x]$ se nazývá $(k,n-k)$**-Padého aproximant** pro g, pokud

- $x \nmid t$ a $\dfrac{r}{t} \equiv g \pmod{x^n}$
- $\deg r < k$, $\deg t \leq n - k$

Obecnější otázkou je hledání Padého aproximantu pro mocninné řady se středem ne nutně v počátku. Tento případ lze však na předchozí převést pomocí substituce. Souvislost s Taylorovým polynomem je zřejmá: pokud g je Taylorova řada zkoumané funkce a r je její Taylorův polynom řádu n, pak $r/1$ je $(n,0)$-Padého aproximant pro g.

Dále řekneme, že $r/t \in F(x)$ je **slabý $(k,n-k)$-Padého aproximant** pro g, pokud

- $r \equiv gt \pmod{x^n}$
- $\deg r < k$, $\deg t \leq n - k$

Podobně jako Cauchyovy interpoanty, i Padého aproximanty lze hledat pomocí věty 3.4:

Důsledek 3.6. *Nechť $g \in F[x]$ je stupeně menšího než $n \in \mathbb{N}$, $k \in \{0,...,n\}$, označme $m = x^n$. Nechť $r,s,t \in F[x]$ je j-tý řádek rozšířeného Eukleidova algoritmu pro m,g, kde j je nejmenší takové, že* $\deg r < k$. *Potom*

(i) r/t je slabý $(k,n-k)$-Padého aproximant pro g. Pokud navíc platí $\gcd(r,t) = 1$, pak (r,t) je $(k,n-k)$-Padého aproximant pro g.

(ii) Pokud $\dfrac{\bar{r}}{\bar{t}} \in F(x)$ je v kanonickém tvaru taková, že $(\bar{r},\bar{t})$ je $(k,n-k)$-Padého aproximant, pak $\bar{r} = \tau^{-1} r$, $\bar{t} = \tau^{-1} t$, kde $\tau = \mathrm{lc}(t) \in F \setminus \{0\}$. Speciálně tedy $(k,n-k)$-Padého aproximant existuje, právě když $\gcd(r,t) = 1$.

Uvedenou větu ilustrujeme na příkladu exponenciální funkce. Předtím ještě poznamenejme, že podle bodu (ii) předchozího důsledku je počet různých Padého aproximantů pro g modulo x^n nejvýše roven počtu dělení v rozšířeném Eukleidově algoritmu. Aby byl tento počet roven n (jako v následujícím příkladu), musí se při každém dělení stupeň snížit o 1.

Úloha 3.3 (5.40)**.** *Aproximujte exponenciální funkci $e^x = 1 + x + x^2/2 + x^3/6 + x^4/24 + ...$ v okolí počátku pomocí racionálních funkcí.*

Řešení. Nejprve spočítáme výstup rozšířeného Eukleidova algoritmu pro $m(x) = x^5$ a $g(x) = x^4/24 + x^3/6 + x^2/2 + x + 1$.

i	r_i	s_i	t_i
0	$m(x)$	1	0
1	$g(x)$	0	1
2	$4x^3+24x^2+72x+96$	1	$-24x+96$
3	$x^2/4+3/2x+3$	$-x/96+1/48$	$x^2/4-3/2x+3$
4	$24x+96$	$x^2/6-x/3+1$	$-4x^3+24x^2-72x+96$
5	1	$-x^3/576-x/72$	$x^4/24-x^3/6+x^2/2-x+1$
6	0	s_6	$-x^5$

Jelikož polynomy t_j nejsou dělitelné x pro žádné $j = 1,...,5$, dostáváme podle předchozího důsledku, že

$$r_1/t_1 = g \text{ je (5,0)-Padého aproximant,}$$

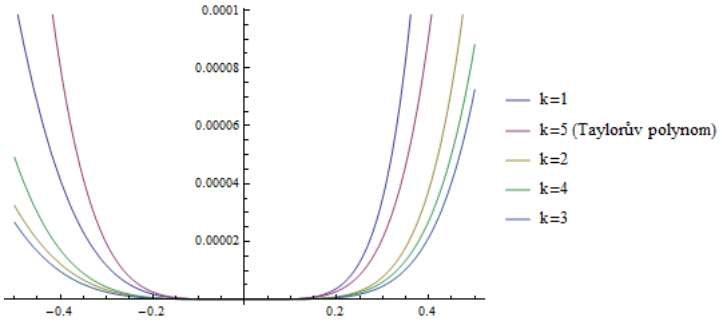
$$\frac{r_2}{t_2} = \frac{-x^3/6-x^2-3x-4}{x-4} \text{ je (4,1)-Padého aproximant,}$$

$$\frac{r_3}{t_3} = \frac{x^2+6x+12}{x^2-6x+12} \text{ je (3,2)-Padého aproximant,}$$

$$\frac{r_4}{t_4} = \frac{-6x-24}{x^3-6x^2+18x-24} \text{ je (2,3)-Padého aproximant a}$$

$$\frac{r_5}{t_5} = \frac{24}{x^4-4x^3+12x^2-24x+24} \text{ je (1,4)-Padého aproximant.}$$

Obrázek 1 zobrazuje absolutní hodnotu rozdílu funkce e^x a $(k,5-k)$-Padého aproximantu na intervalu $(-0.5,0.5)$ pro $k = 1,...,5$. Kromě případu $k = 1$ jsou všechny tyto aproximanty lepší, než Taylorův polynom ($k = 5$). Pro úplnost ještě poznamenejme, že $s_6 = x^4/24+x^3/6+x^2/2+x+1$.



Obrázek 1: Odchylka $(k,5-k)$-Padé aproximantů od exponenciály v okolí počátku.

□

Důsledek 3.6 říká, že řešení problému Padého aproximace je vždy (až na násobek) nějaký řádek rozšířeného Eukleidova algoritmu. Následující příklad se zabývá opačným přístupem: pro která k je daný řádek Eukleidova algoritmu Padého aproximantem?

Úloha 3.4 (5.41)**.** *Nechť $r_j = s_j x^n + t_j g$ je libovolný řádek rozšířeného Eukleidova algoritmu pro dvojici x^n, g, kde $\deg g < n$. Určete, pro která $k \in \{1,...,n\}$ je daný řádek slabým $(k,n-k)$-Padého aproximantem pro g.*

Řešení. Vztah $r_j \equiv gt_j \pmod{x^n}$ zřejmě platí. Dále označme $n_0 = \deg r_0$, $n_1 = \deg r_1$,...,$n_l = \deg r_l$, kde $r_0 = x^n$, $r_1 = g$,...,$r_l = 1$ jsou řádky rozšířeného Eukleidova algoritmu. Aby (r_j,t_j) byl slabým $(k,n-k)$-aproximantem pro g, musí dále platit $\deg r_j < k$, $\deg t_j \leq n-k$. Z podmínky $\deg r_j < k$ plyne $n_j < k$ a dále podle lemmatu 3.2 máme $\deg t_j = n - \deg r_{j-1} = n - n_{j-1}$. Podmínka $\deg t_j \leq n-k$ tedy implikuje $k \leq n_{j-1}$. Nyní je vidět, že řešením jsou právě $k \in \{n_j+1,...,n_{j-1}\}$.

□

3.5 Racionální čínská věta o zbytcích

Větu 3.4 lze formulovat ještě obecněji a rozšířit tak okruh úloh, které díky ní lze řešit. Nejprve uveďme potřebné předpoklady: $m_0,...,m_{l-1} \in F[x]$ jsou nekonstantní, monické, po dvou nesoudělné, $m = m_0...m_{l-1}$ je stupně n, $v_0,...,v_{l-1} \in F[x]$ takové, že $\deg v_i < \deg m_i$ pro $0 \leq i < l$, $k \in \{0,...,n\}$. O dvojici (r,t) polynomů z $F[x]$ budeme mluvit jako o **zobecněné $(k,n-k)$-racionalizaci** polynomů $v_0,...,v_{l-1}$ modulo $m_0,...,m_{l-1}$, pokud

- $gcd(t,m_i) = 1$, $rt^{-1} \equiv v_i \pmod{m_i}$ pro $0 \leq i < l$
- $\deg r < k$, $\deg t \leq n-k$

Pokud $l = 1$, pak nejde o nic jiného, než definici $(k,n-k)$-racionalizace v_0 modulo m_0. Dále řekneme, že (r,t) je **zobecněná slabá $(k,n-k)$-racionalizace** polynomů $v_0,...,v_{l-1}$ modulo $m_0,...,m_{l-1}$, pokud

- $r \equiv tv_i \pmod{m_i}$ pro $0 \leq i < l$
- $\deg r < k$, $\deg t \leq n-k$

Důkaz věty 3.7 je obsahem cvičení 5.42 z [1].

Věta 3.7. *Nechť $m_0,...,m_{l-1} \in F[x]$ jsou nekonstantní, monické, po dvou nesoudělné, $m = m_0...m_{l-1}$ je stupně n, $v_0,...,v_{l-1} \in F[x]$ takové, že* $\deg v_i < \deg m_i$ *pro $0 \leq i < l$, $k \in \{0,...,n\}$. Podle Čínské věty o zbytcích dále existuje polynom $g \in F[x]$ stupně menšího než n takový, že $g \equiv v_i \pmod{m_i}$ pro všechna i. Nakonec ať $r,s,t \in F[x]$ je j-tý řádek rozšířeného Eukleidova algoritmu pro dvojici m,g, kde j je minimální takové, že* $\deg r < k$. *Potom*

(i) *(r,t) je zobecněná slabá $(k,n-k)$-racionalizace polynomů $v_0,...,v_{l-1}$ modulo $m_0,...,m_{l-1}$. Pokud navíc platí $gcd(r,t) = 1$, pak (r,t) je zobecněná $(k,n-k)$-racionalizace polynomů $v_0,...,v_{l-1}$ modulo $m_0,...,m_{l-1}$.*

(ii) *Pokud $\frac{\bar{r}}{\bar{t}} \in F(x)$ je v kanonickém tvaru taková, že $\bar{r},\bar{t} \in F[x]$ je zobecněná $(k,n-k)$-racionalizace polynomů $v_0,...,v_{l-1}$ modulo $m_0,...,m_{l-1}$, pak $\bar{r} = \tau^{-1}r$, $\bar{t} = \tau^{-1}t$, kde $\tau = \mathrm{lc}(t) \in F \setminus \{0\}$. Speciálně tedy zobecněná $(k,n-k)$ racionalizace existuje, právě když $gcd(r,t) = 1$.*

Důkaz. (i) Důkaz je podobný důkazu věty 3.4. Máme $r_j = s_j m + t_j g$, dále pro každé i platí $m \equiv 0 \pmod{m_i}$ a $g \equiv v_i \pmod{m_i}$. Odtud $r_j \equiv t_j v_i \pmod{m_i}$ pro každé i. Pokud navíc $gcd(r_j,t_j) = 1$, pak podle lemmatu 3.1 $gcd(m,t_j) = 1$ a tím pádem $gcd(m_i,t_j) = 1$ pro kažé i. Jelikož jsme j vybrali tak, že deg $r_{j-1} \geq k$, platí i $n - k \geq n - \deg r_{j-1} = \deg t_j$ podle lemmatu 3.2.

K bodu (ii) stačí ověřit, že existuje $s \in F[x]$ takové, že $r = sm + tg$. Zbytek důkazu projde zcela stejně jako ve větě 3.4. Jelikož $rt^{-1} \equiv v_i \pmod{m_i}$ a $g \equiv v_i \pmod{m_i}$ pro každé i, dostáváme z tranzitivity relace $\equiv$, že $rt^{-1} \equiv g \pmod{m_i}$ pro každé i a (jelikož m_i jsou po dvou nesoudělné) $rt^{-1} \equiv g \pmod{m}$. To je ekvivalentní s tím, že $r \equiv tg \pmod{m}$ a odtud již plyne zbytek.

□

Nyní ukážeme, jak lze větu 3.7 využít.

Úloha 3.5 (5.43)**.** *Najděte, pokud existuje, racionální funkci* $\rho = \dfrac{r}{t} \in \mathbb{Q}(x)$ *tak aby*

(a)

$$\rho(-1) = 2,\ \rho'(-1) = 1,\ \rho(1) = -1,\ \rho'(1) = 2,$$
$$\deg r < 1,\ \deg t \leq 3.$$

(b)

$$\rho(-1) = 1,\ \rho(0) = 2,\ \rho(1) = 1,\ \rho'(1) = -1,$$
$$\deg r < 3,\ \deg t \leq 1.$$

Řešení. (a) Pro $l = 2$ budeme hledat zobecněnou (1,3)-racionalizaci pro polynomy $v_0(x) = (x + 1) + 2 = x + 3$, $v_1(x) = 2(x - 1) - 1 = 2x - 3$ modulo $m_0(x) = (x + 1)^2$, $m_1(x) = (x - 1)^2$.

Pomocí čínské věty o zbytcích zjistíme, že pro $g(x) = 3/2x^3 + 1/4x^2 - 3x + 1/4$ platí $g \equiv v_i \pmod{m_i}$, $i = 0{,}1$. Eukleidův algoritmus pro dvojici $m = (x-1)^2(x+1)^2$, g proběhne takto:

i	r_i	s_i	t_i
0	$m(x)$	1	0
1	$g(x)$	0	1
2	$1/36x^2 - 1/2x + 37/36$	1	$-2/3x + 1/9$
3	$432x - 1008$	s_3	$36x^2 + 648x - 108$
4	$1/81$	s_4	$-1/432x^3 - 7/1296x^2 - 1/144x + 1/432$
5	0	s_5	$81x^4 - 162x^2 + 81$

$j = 4$ je nejmenší j takové, že deg $r_j < k = 1$. Zbývá ověřit, že $gcd(r_4,t_4) = 1$, což platí, a (r_4,t_4) je podle předchozí věty zobecněná (1,3)-racionalizace v_0,v_1 modulo m_0,m_1. Snadno se pak ověří, že

$$\rho = \frac{r}{t} = \frac{-16}{3x^3 + 7x^2 + 9x - 3}$$

splňuje podmínky zadání. Pro úplnost doplňme, že $s_3 = -54x - 981$, $s_4 = 1/288x^2 + 5/576x + 61/5184$ a $s_5 = -243/2x^3 - 81/4x^2 + 243x - 81/4$.

Proč tento postup funguje? Nechť $r,t \in F[x]$. Ukážeme, že podmínka

$$\frac{r}{t}(u) = v_0,\ \left(\frac{r}{t}\right)'(u) = v_1, \tag{9}$$

kde $u,v_0,v_1 \in F$, je ekvivalentní s

$$r \equiv vt \pmod{(x-u)^2}, \tag{10}$$

kde $v(x) = v_1(x-u) + v_0$. (10) podle definice znamená $(x-u)^2 \mid v(x)t(x) - r(x)$ a lze ukázat, že to je ekvivalentní podmínce

$$(vt-r)(u) = 0,\ (vt-r)'(u) = 0 \tag{11}$$

Jelikož

$$(vt-r)(u) = v_0t(u) - r(u),$$
$$(vt-r)'(u) = (v't + vt' - r')(u) = v_1t(u) + v_0t'(u) - r'(u),$$

je (11) ekvivalentní

$$\frac{r(u)}{t(u)} = v_0,\ v_1t(u) + \frac{r(u)}{t(u)}t'(u) - r'(u) = 0,$$

což lze napsat též jako

$$\frac{r}{t}(u) = v_0,\ \frac{r'(u)t(u) - r(u)t'(u)}{t^2(u)} = \left(\frac{r}{t}\right)'(u) = v_1.$$

Takto jsme ukázali, že (9) je ekvivalentní (11).

(b) Podobně jako výše lze ukázat, že $\rho = r/t$, $r,t \in \mathbb{Q}[x]$, splňuje podmínky ze zadání, právě když (r,t) je zobecněná (3,1)-racionalizace polynomů v_0,v_1 modulo m_0,m_1, kde

$$m_0(x) = (x+1)x,\ v_0(x) = x+2,$$
$$m_1(x) = (x-1)^2,\ v_1(x) = (-1)(x-1)+1 = -x+2.$$

$v_0(x)$ jsme zvolili nejmenšího stupně tak, aby platilo $v_0(-1) = \rho(-1) = 1$, $v_0(0) = \rho(0) = 2$. Pro $g(x) = 1/2x^3 - x^2 - 1/2x + 2$ platí $g \equiv v_i \pmod{m_i}$, $i = 0,1$. Eukleidův algoritmus pro $m = x(x+1)(x-1)^2$, g proběhne takto:

i	r_i	s_i	t_i
0	$m(x)$	1	0
1	$g(x)$	0	1
2	$2x^2 - 2x - 4$	1	$-2x - 2$
3	1	$-1/4x + 1/4$	$1/2x^2 + 1/2$
4	0	$1/2x^3 - x^2 - 1/2x + 2$	$-x^4 + x^3 + x^2 - x$

Dále $j = 2$ je nejmenší takové, že $\deg r_j < k = 3$. Jelikož však $gcd(r_2,t_2) = gcd(2x^2 - 2x - 4, -2x - 2) = x + 1$, zobecněná (3,1)-racionalizace m_0,m_1 modulo m_0,m_1 podle věty 3.7 neexistuje, a neexistuje tedy ani hledaná funkce ρ.

□

.

Reference

[1] J. Von zur Gathen, J. Gerhard, *Modern Computer Algebra*, Joachim von zur Gathen and Jürgen Gerhard 2013

[2] D. Stanovský, L. Barto, *Počítačová algebra*, Matfyzpress, 2010

[3] D. Stanovský, *Základy algebry*, Matfyzpress, 2010