ZÁPADOČESKÁ UNIVERZITA V PLZNI

FAKULTA PEDAGOGICKÁ

KATEDRA MATEMATIKY, FYZIKY A TECHNICKÉ VÝCHOVY

KRONECKERŮV ALGORITMUS

BAKALÁŘSKÁ PRÁCE

Zdeněk Šuster

Přírodovědná studia, obor Matematická studia

Vedoucí práce: PhDr. Lukáš Honzík, PhD.

Plzeň, 2016

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

V Plzni, 30. června 2016

.....

vlastnoruční podpis

Chtěl bych poděkovat svému vedoucímu bakalářské práce PhDr. Lukáši Honzíkovi, PhD., za odborné vedení, pomoc a rady při zpracování této práce.

Obsah

Úvod

Tato bakalářská práce je zaměřena především na Kroneckerův algoritmus, ale také se budeme zabývat historií podobných algoritmů, Leopoldem Kroneckerem, programem Derive 6, kalkulátorem TI - 92 Plus, faktorizací polynomů. Pro tyto témata je důležitá práce s polynomy, které jsou vysvětleny níže.

Polynom

Pod pojmem polynom nebo také mnohočlen budeme rozumět výraz zadaný v následujícím tvaru:

„$p(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = \sum_{i=0}^{n} a_i x^{n-i}$“, kde konstanty $a_0,\ldots,a_n$ jsou koeficienty ($a_n \neq 0$), které mohou představovat libovolná celá čísla, a n je stupeň polynomu, přičemž $n \in N$, dále x je proměnná a a_0 absolutní člen.

Uveďme na příkladu $4x^2$, kde koeficient je 4, proměnná x a exponent 2.

V případě Kroneckerova algoritmu, jak je níže popsáno, se nacházíme v oboru celých čísel (**Z**).

Rozdělení polynomů

Reducibilní polynom - tj. polynom f(x), který jde zapsat jako součin dvou polynomů menšího stupně než f(x).

Příklad:

$x^2 - 4 = (x - 2) \cdot (x + 2)$

Ireducibilní polynom - tj. polynom f(x), který již nejde zapsat jako součin dvou polynomů menšího stupně než f(x).

Příklad:

$x^2 + 4$ - již dále nejde rozložit

Příklad:

$x^2 - 2$ = opět nejde dále rozložit v polynomech s celočíselnými koeficienty (v reálných číslech lze)

Stupeň polynomu p(x)

Stupeň polynomu lze chápat jako nejvyšší exponent proměnné *x* s nenulovým koeficientem, který značíme *st p(x)*.

Znázornění na jednoduchých příkladech:

a) $p(x) = 4$, kde je stupeň konstantního polynomu roven 0

b) $p(x) = x + 3$, kde je stupeň lineárního polynomu roven 1

c) $p(x) = x^2 - 2x$, kde je stupeň kvadratického polynomu roven 2

d) $p(x) = x^n \pm c$, kde n je stupeň n-tého polynomu roven n, a c je libovolné reálné číslo (konstanta)

Kořen polynomu

Nechť kořenem polynomu rozumíme číslo λ, pokud platí:

$P(\lambda) = 0$

Pro rovnice typu $P(x) = 0$ je řešením právě kořen polynomu p(x), a také je pro ně známa základní algebraická věta, která je definována následovně:

„$P(x) = a_n \cdot x^n + \ldots + a_0$ je polynom s koeficienty $a_0, \ldots, a_n \in \mathbf{C}$, $a_n \neq 0$ stupně $n \geq 1$. Pak existuje číslo $a \in \mathbf{C}$, že $P(a) = 0$.“

A dále vyjadřuje:

*„Každý polynom stupně $n \geq 1$ má v **C** alespoň jeden kořen.“*

Vlastnosti

a) Pokud λ je kořenem polynomu P(x) stupně $n \geq 1$, potom $P(x) = (x - \lambda) \cdot g(x)$, kde g(x) je polynom stupně n-1.

b) Z předchozí vlastnosti plyne, že pokud známe k kořenů polynomu n-tého stupně, můžeme opakovaným způsobem z rozkladu $P(x) = (x - \lambda) \cdot g(x)$ rozložit libovolný polynom P(x) na součin kořenových činitelů, které již známe z předchozí vlastnosti, a polynomu g(x) stupně n-k, tedy platí:

$P(x) = P(x) = (x - \lambda_1) \cdot (x - \lambda_2) \ldots (x - \lambda_k) \cdot g(x)$, kde λ_i jsou známé kořeny polynomu P(x) a členy $(x - \lambda_i)$ jsou kořenovými činiteli.

Polynom g(x) lze poté získat z polynomu P(x) jeho vydělením výrazem $(x - \lambda_1) \ldots (x - \lambda_k)$.

c) Kořeny zjistíme jen u reducibilního polynomu (mnohočlenu).

Příklad:

Mějme zadaný polynom $f(x) = x^2 - 2x + 1$. Zjistěte kořeny a kořenové činitele.

Tento polynom lze rozložit na kořenové činitele $(x - 1) \cdot (x - 1)$. Tudíž je patrné, že kořeny $\lambda_1, \lambda_2 = 1$.

Operace s polynomy

Rovnost

Polynomy P(x) a Q(x) se rovnají, pokud platí $P(\alpha) = Q(\alpha)$, tj. právě tehdy, když mají stejné koeficienty u stejných mocnin proměnné x, kde všechna α jsou komplexní nebo reálné čísla. Z rovnosti vyplývá operace sčítání a odečítání. Při těchto operacích s dvěma a více stejnými proměnnými se stejnými exponenty lze tyto proměnné posléze od sebe sčítat nebo odečítat.

Součet/rozdíl

Pro součet a podíl zní definice takto: *„Součet i rozdíl polynomů P(x) a Q(x) stupňů m,n je polynomem stupně, který je menší nebo roven většímu z čísel m,n.“* Lze matematicky zapsat takto: $(st(P(x) \pm Q(x)) \leq max(m,n))$.

Z definice plyne, že součet i rozdíl polynomů je vždy polynom, ale také může být ve výsledku konstanta. Ilustrace na následujících příkladech:

a) $x + x = 2x$

b) $4x^2 - 3x^2 = x^2$.

c) $(2x + 1) - 2x = 1$

Dále také je třeba uvést, že rozdíl dvou polynomů, které se rovnají, je nulový polynom.

Součin

Operace součin je matematicky vysvětlována následovně:

Součin polynomů stupňů m a n je polynom stupně m + n, z toho lze usoudit, že součin dvou nenulových polynomů je nenulový polynom.

Příklad:

$x^2 \cdot x^3 = x^{2+3} = x^5$

Podíl

Podíl lze chápat takto:

Podíl polynomů stupňů m a n je polynom stupně m - n.

Příklad:

$x^8/x^5 = x^{8-5} = x^3$

Také tuto metodu lze řešit několika způsoby, např. Hornerovo schéma a dělení mnohočlenů mnohočlenem se zbytkem. Hornerovo schéma neboli také Hornerův algoritmus je nenáročná metoda pro dělení mnohočlenů. Tato metoda je znázorněna na následujícím příkladu.

Příklad:

Mějme $f(x) = x^3 - 6x^2 + 12x - 16$ a vydělme f(x) výrazem (x - 4).

x_0	x^3	x^2	x^1	x^0
4	1	-6	12	-16
		4	-8	16
g(x)	1	-2	4	0

=> výsledkem tedy bude $g(x) = x^2 - 2x + 4$

Dělitelem je (x - 4), z toho plyne, že $x_0 = 4$. Dále na zbylé pozice v prvním řádku Hornerova schématu zapíšeme počet jednotlivých polynomů dle stupně. Následně číslo x_0 násobíme tolikrát, kolikrát se daný polynom v daném výrazu nachází. Zde je to jedenkrát a číslo 1 se zapíše do posledního řádku pro zjištění výrazu po dělení mnohočlenů. Poté se výsledek tohoto součinu zapíše do poslední řádku, napíše do třetího sloupce a opět se udělá součet ve sloupci a vyjde -2. Tento proces se opakuje do zjištění nulového zbytku.

Další metodou, kterou lze znázornit, je dělení mnohočlenu (polynomu) mnohočlenem (polynomem) se zbytkem nebo beze zbytku. Lze ji ilustrovat na následujícím příkladu.

Příklad:

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

$-x^2 + x$

$x - 1$

$x - 1$

0

Výše uvedený postup je velice prostý. Vezmeme-li první člen prvního mnohočlenu x^2 a vydělíme ho s prvním členem druhého mnohočlenu x, poté výsledek tohoto podílu napíšeme do výsledku příkladu, tj. x, kde nám vyjde daný výraz po zjištění daného zbytku. Poté zpětně daný výsledek podílu vynásobíme výrazem (x - 1) a budeme ho odečítat od

prvního mnohočlenu s vyšší mocninou. Dále mějme výsledek rozdílu x - 1. Z tohoto výsledku vezmeme první člen tohoto mnohočlenu x a opět ho vydělíme prvním členem druhého mnohočlenu x a výsledek 1 následně zapíšeme do výsledku tohoto příkladu x + 1. Dále číslo 1 vynásobíme výrazem (x - 1) a výsledek tohoto součinu (x - 1) zapíšeme opět níže pod výsledné výrazy. Následně výrazy (x - 1) od sebe odečteme a vyjde nulový zbytek. Z toho je patrné, že $f(x) = (x^2 - 1)$ lze rozložit na $(x - 1) \cdot (x + 1)$.

Umocnění

Je také zapotřebí zmínit, jak se polynomy chovají při **umocnění**. Lze ilustrovat na tomto příkladu: $(x^2)^2 = x^{2 \cdot 2} = x^4$.

Historický rámec, vybrané předchozí a následující algoritmy

Před vznikem Kroneckerova algoritmu již existovala řada metod či algoritmů pro faktorizaci polynomů neboli řešení polynomiálních rovnic v oblasti algebry. První zmínka o těchto metodách je zaznamenána už v letech 1900 – 1600 př. n. l., kdy Babyloňané využívali nejprve hledání kořenových činitelů, ale také znali již algoritmus, který vedl k vyřešení kvadratických rovnic, a posléze zvládli vyřešit numericky kubické rovnice.

Po Babyloňanech následovala odmlka s tématem o řešení polynomiálních rovnic, ale po dlouhé době navázali na Babyloňany italští matematici v období renesance s tématem řešení kubických rovnic. Poté měl vývoj ohledně polynomiálních rovnic vzestupnou tendenci. S novými elegantními metodami přišli Isaac Newton, Francois Viéte, Pierre Fermat, Karl Friedrich Gauss. S rozklady mnohočlenů se zabýval jak Francois Viéte, tak i Karl Friedrich Gaus. Francois Viéte přišel na závislost mezi kořeny mnohočlenů a hodnotami jejich koeficientů. Za to práce Karla Friedricha Gausse nebyla tak významnou ve společnosti, jelikož byla zapomenuta, ale poté objevena. Za vznikem známé Fermatovy věty stojí Pierre Fermat. Tato věta vyjadřuje: *„$x_p - x = \prod (x-a)$, $a \in Zp$, p je prvočíslo“*. Dalším matematikem, který přispěl do této tématiky, je Isaac Newton, který objevil metodu aproximace reálných kořenů polynomů.

Dále William George Horner na začátku 19. století popsal algoritmus, který je po něm pojmenován, ale již dříve byl znám Isaacu Newtonovi a dokonce již ve 13. století

čínskému matematikovi Ch'in Chiu-Shao. Tento Hornerův algoritmus (neboli schéma) je optimální existující algoritmus na vyhodnocování polynomů v reálných číslech. Dále v roce 1793 Hermann Schubert objevil jako první algoritmus pro faktorizaci polynomů (tj. proces, jak vyjádřit polynom s koeficienty v daném oboru nebo v celých číslech jako součin ireducibilních faktorů s koeficienty ve stejném oboru). Dále stojí za zmínku Eisensteinovo kritérium ireducibility polynomu v Z[x], které lze využít pro rozdělování polynomů na třídy rozložitelných a nerozložitelných mnohočlenů. Pro pochopení tohoto kritéria a další práci s polynomy lze ilustrovat nejprve na následujícím zadefinování ireducibilního polynomu a uvedení jednoduchých příkladů na toto kritérium. Definice ireducibilního polynomu zní takto: „*Polynom P(x) nad tělesem T je ireducibilní v tělese T, pokud jej není možné rozložit na součin polynomů R(x), S(x) nad T stupně alespoň prvního. Takže nemůže platit P(x) = R(x)·S(x).*“ Z této definice je patrné, že $f(x) = x^2 + 4$ je ireducibilní nad tělesem R, jelikož nelze dále rozložit na součin polynomů R(x) a S(x). Opakem tohoto polynomu je reducibilní polynom, který dle logického úsudku jde dále rozložit na součin polynomů R(x) a S(x). Například $f(x) = x^2 - 4$ jde rozložit na $(x - 2) \cdot (x + 2)$, tj. reducibilní. Dále také u těchto polynomů lze vytknout celé číslo kromě ±1. Zde se jedná pouze o metodu zjištění společného největšího dělitele koeficientů polynomů a samozřejmě rozkladu. Například lze tuto metodu znázornit na $f(x) = 4x^2 - 64x + 16$, a to lze zapsat jako $4*(x^2 - 16x + 4)$.

Až po těchto matematicích, v roce 1882, Leopold Kronecker přišel na algoritmus pro faktorizace polynomu, pomocí kterého lze určit rozklad libovolného polynomu Z[x] (neboli ireducibilní polynom). Tímto tak rozšířil Schubertův algoritmus, zpřístupnil rozklad polynomů vyšších mocnin. Po tomto algoritmu udělal významný krok v matematice Kurt Hensel, který byl mimo jiné studentem Leopolda Kroneckera a také editoval a shromáždil 5 svazků z jeho prací. Také přišel na důležitý algoritmus, který je nazýván Henselovo zdvižení. Pomocí tohoto algoritmu s propojením Berlekampova algoritmu lze nalézt rozklad mnohočlenu nad konečnými tělesy, tímto je nejlepším faktorem pro řešení faktorizace polynomů.

V druhé polovině 20. století přišel Bill Gosper na algoritmus, který byl prvním sumačním algoritmem na světě. Jeho důležitou součástí je řešení rekurenční relace pro hypergeometrické polynomy. V tomto období byl také objeven Berlekampův algoritmus

pro faktorizaci polynomů nad konečným tělesem, a to Elwynem Berlekampem, ale na tomto algoritmu měli zásluhu i dva českoslovenští matematici Karel Petr a Štefan Schwarz.

Mezi další algoritmy, které jsou specifické pro práci s polynomy, patří Musserův algoritmus, Tobeyho-Horowitzův algoritmus a Yunův algoritmus. Tyto algoritmy fungují na metodě Square-free decomposition nebo také rozklad polynomu v součin faktorů nedělitelných čtvercem, tj. je druh rozkladu polynomu.

Leopold Kronecker

obr. 1

Leopold Kronecker, který přišel na algoritmus pro faktorizaci polynomů, se narodil v pruském Liegnitzu 7. prosince 1823 rodičům Isidoru Kroneckerovi a Johanne Prausnitzerové, kteří byli židovského původu. Toto náboženství Leopold také přijal, ale na sklonku života začal uznávat křesťanství. S rodiči byl považován za velmi zámožnou rodinu i díky úspěšnosti svého otce v oblasti obchodu. Do 15 let byl jediným potomkem svých rodičů, ale o rok později se narodil druhorozený bratr Hugo Kronecker, který byl považován za významného fyziologa. Své zaujetí pro matematiku získal zásluhou domácích učitelů, které si jeho rodiče objednávali na soukromé hodiny. Leopoldův talent na matematiku objevil na Liegnitzském gymnáziu Ernst Eduard Kummer, který jej vyučoval, vkládal do něj naděje a byl jeho životním přítelem.

Jeho vysokoškolská studia odstartovala v roce 1841, kdy se přihlásil na Berlínskou univerzitu, kde se nezabýval jen matematikou, ale také i jinými oblastmi jeho zaměření, jako například chemií, astronomií, meteorologií a mimo jiné i filozofií. Mezi jeho významné učitele na této univerzitě jsou považováni Dirichlet a Steiner. V období jednoho roku, tj. v letech 1843 – 1844, vycestoval během svého studia na studijní pobyty na univerzity v Bonnu a Vratislavi.

Poté se vrátil zpět do Berlína, kde promoval s prací o Komplexních jednotkách, a začal pracovat na své doktorské práci pod vedením Johanna Dirichleta na téma Algebraická teorie čísel. I když se stále mohl věnovat studiu v Berlíně, tak na necelých 10 let opustil akademickou sféru a věnoval se osobním záležitostem. Pronikl do oblasti obchodu a získal natolik finančních prostředků i zásluhou sňatku s dcerou svého bohatého strýce, že peníze nebyly důležitým aspektem, na které by bral ohled. Po této necelé desetileté etapě života, v roce 1853, se vrátil na akademickou půdu do Berlína, kde spíše chtěl spolupracovat s ostatními místními významnými matematiky než dosahovat akademických titulů. V tom samém roce také rozšířil Galoisovu teorii algebraických rovnic. Dále publikoval nespočet prací v oblasti algebry a díky tomu byl v roce 1861 zvolen do Berlínské akademie věd. I když nebyl zaměstnancem této univerzity, měl právo zde přednášet. Vyučoval zde teorii čísel, teorii rovnic, teorii determinantů a integrálů. Svými matematickými postupy a myšlenkami nepřitahoval příliš studentů, jen jejich menší část dokázala jeho úvahám porozumět, do které patřili například Georg Cantor a Edmund Husserl. Názorný příklad jeho myšlenek lze ilustrovat na jeho výroku: *„Bůh stvořil celá čísla, vše ostatní je dílem člověka.“*

Měl také zásluhy a vysoké postavení v Crellově matematickém časopise, kde pracoval jako editor. Ke zvýšení jeho matematického postavení v Německu napomohlo získání akademického titulu profesor v roce 1883 po svém bývalém učiteli Ernstu Eduardovi Kummerovi, ale větší význam mělo jeho jmenování do Královské společnosti v Londýně na konci ledna roku 1884. Ve svých 68 letech (29. prosince 1891) umírá v Berlíně o pár měsíců déle než jeho manželka.

Teoretický základ Kroneckerova algoritmu

Algoritmus, který umožňuje v konečném počtu kroků rozhodnout jako tento, zda je daný polynom f(x) stupně n s celočíselnými koeficienty dělitelný nějakým polynomem g(x) rovněž s celočíselnými koeficienty, 0 < st g(x) < n, či zda žádný takovýto dělitel neexistuje. Postup tohoto algoritmu je znázorněn do 5 kroků, které jsou na sebe závislé a tvoří posloupnost:

1. Při hledání jistého dělitele g(x) s celočíselnými koeficienty dochází k možnosti omezení se na polynomy, pro které je stupeň menší nebo roven číslu s=$[\frac{n}{2}]$, kde $[\frac{n}{2}]$

je tzv. celá část čísla $\frac{n}{2}$, tj. největší celé číslo, které je menší nebo rovno $\frac{n}{2}$. Pro pochopení lze ilustrovat na následujícím stručným příkladu. Pokud se např. n = st *f(x)*=11, je s = $[\frac{11}{2}]$= 5.

2. V dalším kroku vypočteme s+1 funkčních hodnot polynomu *f(x)*. Zde je ze začátku obvyklé si zvolit x = 0, 1, . . ., s. Poté získáme celočíselné funkční hodnoty *f(0)*, *f(1)*, *f(2)*, . . ., *f(s)*.

3. Je-li polynom *f(x)* dělitelný polynomem *g(x)*, musí funkční hodnota *g(0)* dělit *f(0)*, *g(1)* dělit *f(1)*, . . ., *g(s)* dělit *f(s)*. Díky tomu lze utvořit množiny $D_{f(0)}$, $D_{f(1),\ldots,}$ $D_{f(s).}$ Pokud by se ale *f(k)* = 0 pro některé k = 0, 1, . . ., s, bylo by číslo k kořenem polynomu *f(x)* a *g(x)* = x – k by byl kořenovým činitelem a tato úloha by byla vyřešena. Z toho plyne předpoklad, že *f(k)* ≠ 0 pro všechna k = 0, 1, . . ., s a množiny $D_{f(k)}$ jsou tím pádem konečné.

4. Pro každou s + 1-tici čísel *g(0)* ∈ $D_{f(0)}$, g(1) ∈ $D_{f(1)}$, . . ., g(s) ∈ $D_{f(s)}$ nalezneme takový (interpolační) polynom *g(x)*, který nabývá v bodech x = 0, 1, . . ., s předepsaných hodnot *g(0)*, *g(1)*, . . ., *g(s)*. Tento polynomu *g(x)* vždy existuje a je právě jeden. Lze ho také nazvat Newtonovým interpolačním polynomem a přijít na něj z tvaru: *g(x)* = α_0+ $\alpha_1(x-a_0)$+ $\alpha_2(x-a_0)(x-a_1)$+…+ $\alpha_s(x-a_0)\ldots(x-a_{s-1})$. Poté je za potřebí ještě vypočítat koeficienty α_0, α_1,…, α_s, kde se zvolí a_0, a_1,…, a_s jako posloupnost po sobě jdoucích celých čísel (a_i = i, kde i = 0, 1,…, s). A dále se označí *g(a_i)* = b_i pro i = 0, 1,…, s, z čehož je možno sestavit tzv. „schéma rozdílů“, kde platí $\Delta b_i = b_{i+1} - b_i$, pro i = 0, 1,…, s – 1; $\Delta^2 b_i = \Delta b_{i+1} - \Delta b_i$;…

b_0
Δb_0
b_1 $\Delta^2 b_0$
Δb_1 .
b_2 $\Delta^2 b_1$.
Δb_2 .
b_3 .
.
.

Pro koeficienty α_k poté platí $\alpha_k = \frac{\Delta^k b_0}{k!}$ a dále platí pro označení b_s = *g(s)*.

5. Pokud je opravdu *g(x)* polynom s celočíselnými koeficienty, 1 ≤ st *g(x)* ≤ s, potom lze vyzkoušet, zda *g(x)* dělí *f(x)*. Pokud ano, je úloha vyřešená a získáme rozklad tvaru *f(x)* = *g(x)*h(x)*, kde *g(x)* a *h(x)* ∈Z[x], st *g(x)* > 0 a st *h(x)* > 0. V nepříznivém případě se vrátíme k bodu 4 a celý postup se zopakuje pro další s + 1-tici *g(0)*, *g(1)*, . . ., *g(s)*.

Celý postup tohoto algoritmu je znázorněn na diagramu (viz obr. 2), který je umístěn v příloze této práce. Pro znázornění a pochopení jednotlivých bodů Kroneckerova algoritmu, které jsou popsány již výše, následuje jednoduchý příklad.

Vzorový příklad

Rozhodněte o reducibilitě nebo ireducibilitě polynomu f(x) = $2x^2 + 8x + 8$ v Z[x].

1. Ze zadání je patrné, že stupeň polynomu n = st *f(x)* = 2, tj. nejvyšší mocnina neznámé x, a dále že s = $[\frac{2}{2}]$ = 1, tj. celá část čísla $\frac{n}{2}$. Z toho plyne, že g(x) je nanejvýše lineární polynom tj. *g(x)* = ax + b.

2. Pro výpočet s + 1 funkčních hodnot mějme x = 0 a 1 (lze zvolit i jiná celá čísla jako funkční hodnoty), a tím získáme celočíselné funkční hodnoty *f(0)* = 8 a *f(1)* = 18.

3. Vytvoříme množiny všech jejich celočíselných dělitelů.
   $D_{f(0)}$ = {1, -1, 2, -2, 4, -4, 8, -8};
   $D_{f(1)}$ = {1, -1, 2, -2, 3, -3, 6, -6, 9, -9, 18, -18}.

4. Pro každou s + 1-tici čísel *g(0)* ∈ $D_{f(0)}$ a g(1) ∈ $D_{f(1)}$ nalezneme takový (interpolační) polynom *g(x)*, který v bodech x = 0 a 1 nabývá hodnot *g(0)* = 4 a *g(1)* = 6. K nalezení Newtonova interpolačního polynomu je za potřebí „schéma rozdílu“, do kterého dosadíme hodnoty *g(0)* a *g(1)*,a které vypadá takto:

   4
   2
   6

   Poté zde dostáváme koeficienty:

   $\alpha_0 = \frac{4}{0!} = 4$

   $\alpha_1 = \frac{2}{1!} = 2$

Tudíž z předepsaného tvaru pro $g(x) = \alpha_0 + \alpha_1(x - a_0) + \alpha_2(x - a_0)(x - a_1) + \ldots + \alpha_s(x - a_0)\ldots(x - a_{s-1})$ dostáváme:

$g(x) = 4 + 2(x - 0) = 2x + 4$

Jelikož se jedná o vzorový příklad, nebudou zde vypsány všechny možné kombinace eventuálních funkčních hodnot polynomu g(0) a g(1).

5. Polynom $g(x)$ splňuje podmínku, že má celočíselné koeficienty, $1 \leq st\ g(x) \leq s$, poté tedy lze vyzkoušet, zda $g(x)$ dělí $f(x)$. Pokud ano, tak zbytek při dělení mnohočlenů bude nulový a pokud ne, tak naopak. V předchozím kroku vyšel člen 2x + 4, kterým bude vydělen původní polynom f(x).

   $(2x^2 + 8x + 8)/2x + 4 = x + 2$

   $-\ 2x^2 - 4x$

   $4x + 8$

   $-\ 4x - 8$

   0 => nulový zbytek => g(x) dělí f(x) => získáme rozklad tvaru $f(x) = g(x)*h(x)$, kde $g(x)$ a $h(x) \in Z[x]$. Tímto algoritmus končí a můžeme říci, že polynom f(x) je reducibilní.

Praktické využití, řešené příklady

Tato kapitola je hlavně zaměřena na praktické využití Kroneckerova algoritmu a také počítání s polynomy, které jsou více probrány v úvodu této práce. Jsou zde ukázány různorodé příklady od nejlehčích až po nejtěžší, které jsou všechny počítány v Z[x] (tj. podmínka Kroneckerova algoritmu), ale také se zde lze setkat z programem Derive 6, kalkulátorem TI - 92 Plus od společnosti Texas Instruments. Tyto matematické pomůcky pracují na bázi Kroneckerova algoritmu pro méně i více složitější příklady na faktorizaci polynomů. Dále také použít pro řešení příkladů na faktorizaci polynomů online webové prostředí WolframAlpha. Tato pomůcka pro rozklad polynomů bohužel nepracuje na bázi Kroneckerova algoritmu, ale na bázi sofistikovanějších algoritmů (viz kapitola WolframAlpha).

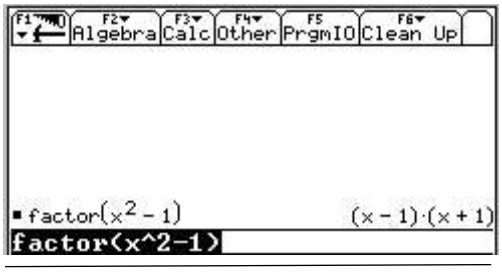
Praktické využití

Kalkulátor TI - 92 Plus

Kalkulátor TI - 92 Plus, který vyšel na trh v roce 1999, má mnoho matematických funkcí pro počítání daných složitých příkladů. Například počítání s polynomy, vykreslování grafů funkcí, integrace, limity, řady apod. Její design je vyobrazen na obr.3 v příloze. Pomocí vybraného kabelu (černý/stříbrný) a programu TI - Graph Link 89, který je taktéž kompatibilní s tímto kalkulátorem, lze exportovat požadované zadání i výsledek daného příkladu do počítače. Pomocí rozsáhlé klávesnice tohoto kalkulátoru lze během krátké doby vyřešit zadaný příklad v závislosti na jeho náročnost. Ale samozřejmě že nedokáže vyřešit hodně rozsáhlé příklady, například u vícestupňových polynomiálních rovnic. Proto existují matematické programy, které tyto příklady dokáží vyřešit, jako je například Derive 6, který je taktéž popsán níže. Zde následuje několik příkladů na faktorizaci polynomů, které tento kalkulátor dokáže i nedokáže vyřešit podle náročnosti daného příkladu. Pro zadání daného příkladu nejprve zapneme kalkulátor a poté stisknutím tlačítka F2 vybereme příkaz *„factor“* stisknutím čísla 2. Pokud je zcela zaplněna pracovní obrazovka kalkulátoru, stačí stisknutím tlačítka F1 a příkazem *„clear home“*, který vyvoláme stisknutím čísla 8, vymazat zaplněnou pracovní obrazovku předchozími příklady. Níže jsou znázorněny příklady lehčí a poté postupně bude růst jejich náročnost výpočtu pro tento kalkulátor.

Příklad 1

Mějme polynom $f(x) = x^2 - 1$. Je polynom f(x) reducibilní nebo ireducibilní?

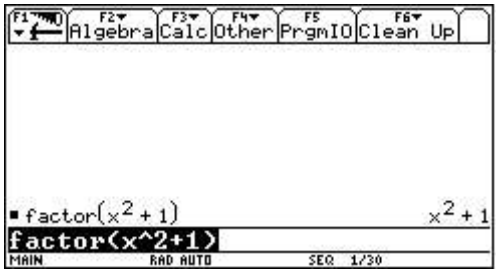


obr.4

Z obrázku je patrné, že nám kalkulátor TI - 92 Plus rozložil polynom $f(x) = x^2 - 1$ na dva členy (x - 1) a (x + 1). Díky tomu zjištění můžeme říci, že polynom f(x) je reducibilní.

Příklad 2

Mějme polynom f(x) = x^2 + 1. Je polynom f(x) reducibilní nebo ireducibilní?

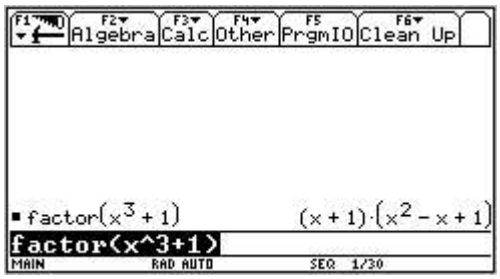


obr.5

Po změnění znaménka u mnohočlenu z předchozího příkladu lze zjistit, že polynom je ireducibilní.

Příklad 3

Je zadán polynom f(x) = x^3 + 1. Zjistěte, zda je zadaný polynom rozložitelný či nerozložitelný.

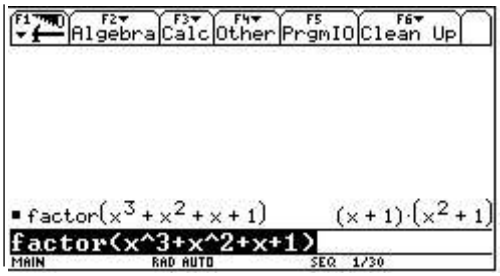


obr.6

Dle kalkulátoru se rozklad polynomu f(x) skládá z těchto mnohočlenů (x + 1) · (x^2 - x + 1), tudíž zadaný polynom je rozložitelný, tedy reducibilní.

Příklad 4

Zjistěte, zda polynom f(x) = x^3 + x^2 + x + 1 je reducibilní či ireducibilní.

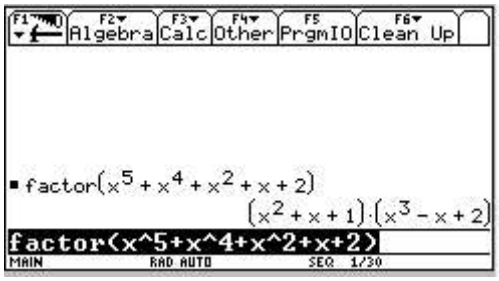


obr.7

Opět se jedná o reducibilní polynom f(x), který kalkulátor vyřešil, a je rozložený na mnohočleny $(x + 1) \cdot (x^2 + 1)$.

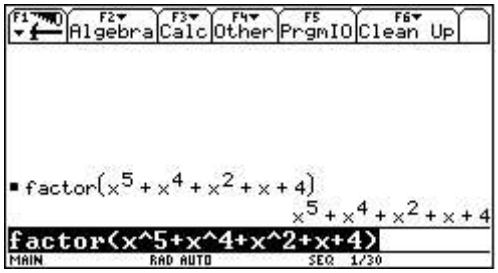
Příklad 5

Mějme zadaný polynom pátého stupně $f(x) = x^5 + x^4 + x^2 + x + 2$. Je zadaný polynom reducibilní nebo ireducibilní?

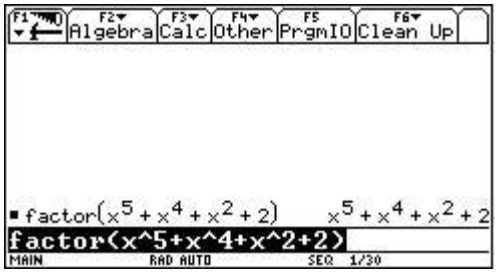


obr.8

Zde je patrné, že je opět polynom f(x) reducibilní, tedy rozložitelný na $(x^2 + x + 1) \cdot (x^3 - x + 2)$, ale stačí si zvolit jiný absolutní člen nebo vynechat v zadání lineární člen, a ihned je polynom f(x) ireducibilní (viz níže).



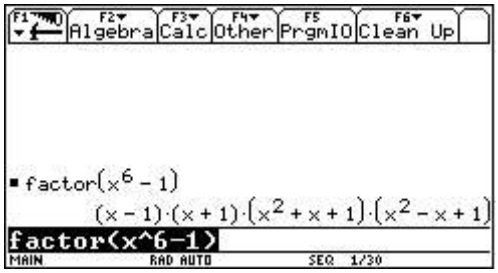
obr.9



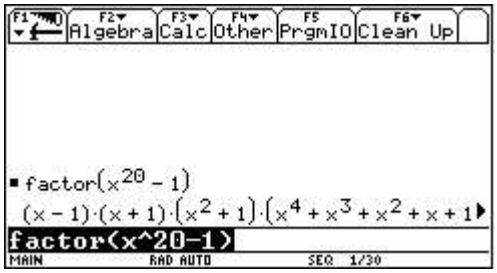
obr.10

Příklad 6

Jsou zadané polynomy $f(x) = x^6 - 1$ a $g(x) = x^{20} - 1$. Máme rozhodnout, zda jsou tyto polynomy reducibilní nebo ireducibilní.

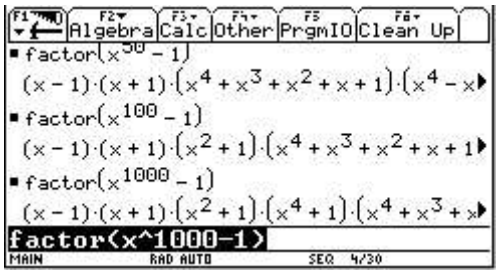


obr.11

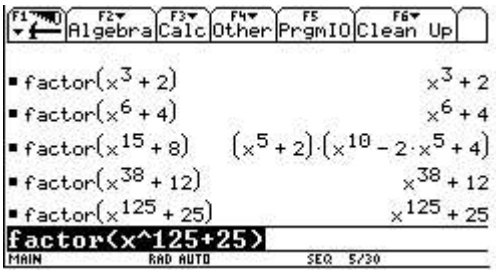


obr.12

Polynom f(x), který je rozložen na mnohočleny $(x - 1) \cdot (x + 1) \cdot (x^2 + x + 1) \cdot (x^2 - x + 1)$, a také polynom g(x), který je rozložitelný na $(x - 1) \cdot (x + 1) \cdot (x^2 + 1) \cdot (x^4 + x^3 + x^2 + x + 1) \cdot (x^4 - x^3 + x^2 - x + 1) \cdot (x^8 - x^6 + x^4 - x^2 + 1)$, jsou reducibilní. Z tohoto příkladu plyne, že pokud je zadaný polynom n-tého stupně v řádu desítek až stovek (viz obr. 13) s absolutním celočíselným členem, tak pokaždé kalkulátor TI - 92 Plus je schopen podobný příklad vyřešit, i když je reducibilní či ireducibilní. Důkaz tohoto tvrzení lze demonstrovat na následujících obrázcích.



obr.13



obr. 14

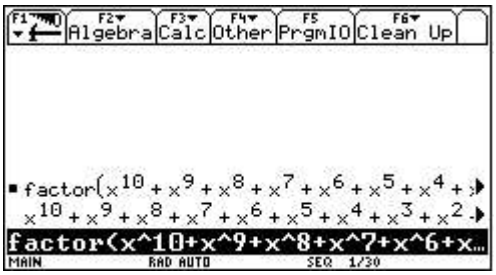
Příklad 7

Mějme zadané polynomy:

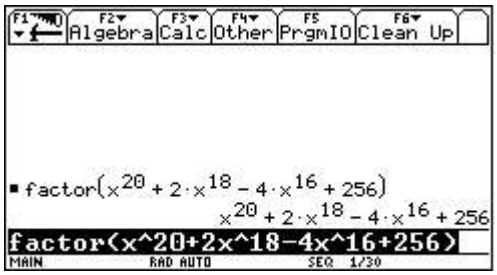
$f(x) = x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 2$

$g(x) = x^{20} + 2x^{18} - 4x^{16} + 256$

Zjistěte, zda zadané polynomy jsou reducibilní či ireducibilní.



obr.15



obr.16

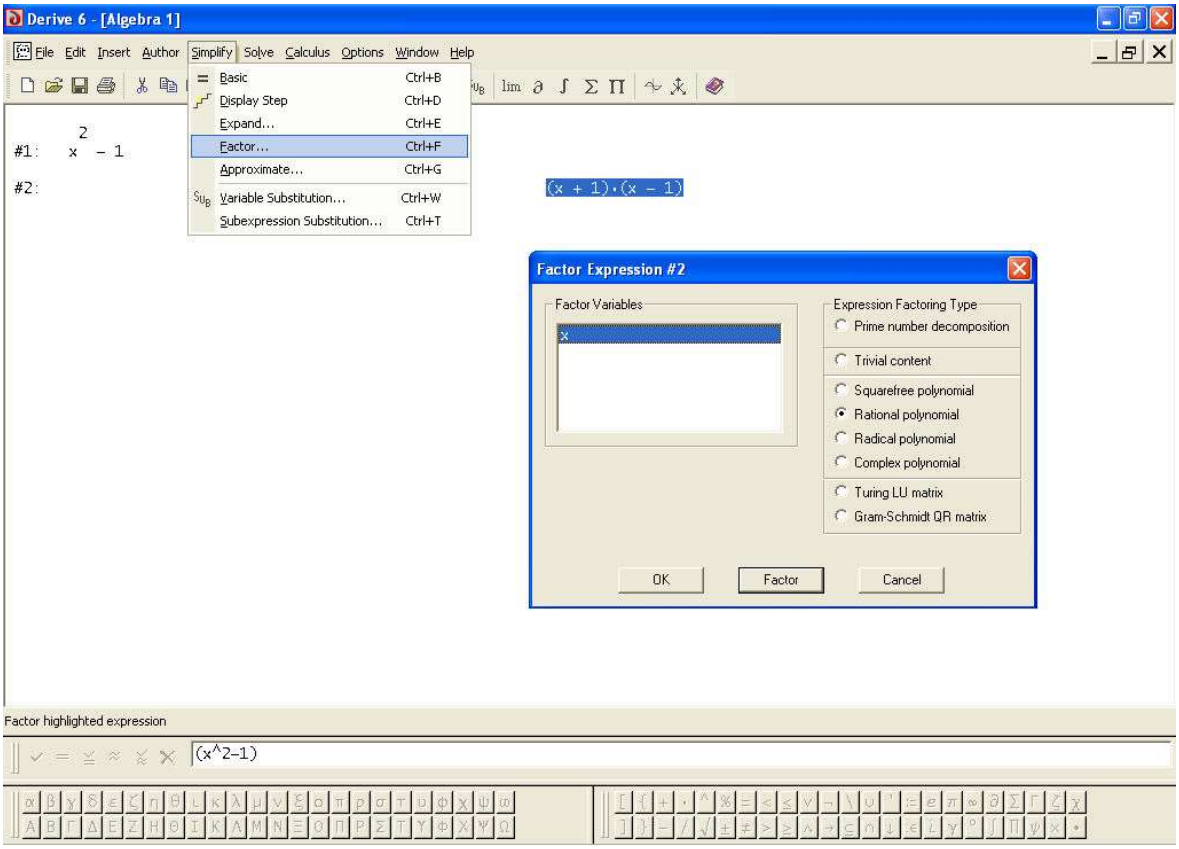
Jak je na první pohled patrné, kalkulátor již nedokázal rozložit zadané polynomy f(x) a g(x). Z předchozích příkladů, u kterých si lze všimnout, že i pokud je zadaný polynom s velmi vysokým stupněm a absolutním členem, tak kalkulátor daný polynom zvládne vyřešit. Ale pokud se těchto členů s vyšším stupněm nachází v zadaném polynomu vícero, tak nejspíše díky nedostatku paměti či kapacity tento kalkulátor nedokáže vypočítat zadané rozsáhlé polynomy. Proto tento typ kalkulačky a jiné podobné typy dokáží efektivně vyřešit přibližně polynomy šestého možná i sedmého stupně s nízkými celočíselnými koeficienty.

Derive 6

Derive 6 je rozsáhlý matematický program od společnosti Texas Instrument, který byl vydán v roce 2004. Není kompatibilní již s novými verzemi Windows, ale má jednoduché prostředí a design. Díky své jednoduchosti je možno využít řadu jednoduchých mechanismů k řešení i složitých příkladů pomocí daných příkazů pro řešení zadaného příkladu (např. integrace, derivování, faktorizace polynomů). Pro toto téma je nejdůležitější faktorizace polynomů, která je znázorněna na následujících příkladech. Řešení daného příkladu lze docílit nejprve zapsáním daného polynomu, poté přechodem na kartu *„simplify“* označíme příkaz *„faktor“*. Dále po zobrazení různých možností pro výpočet výsledku stisknutím pole *„factor“* nám Derive 6 faktorizuje zadaný polynom. Postup zadávání těchto příkazů je zobrazen v příkladu 1.

Příklad 1

Mějme tedy zadaný polynom $f(x) = x^2 - 1$. Je reducibilní nebo ireducibilní?

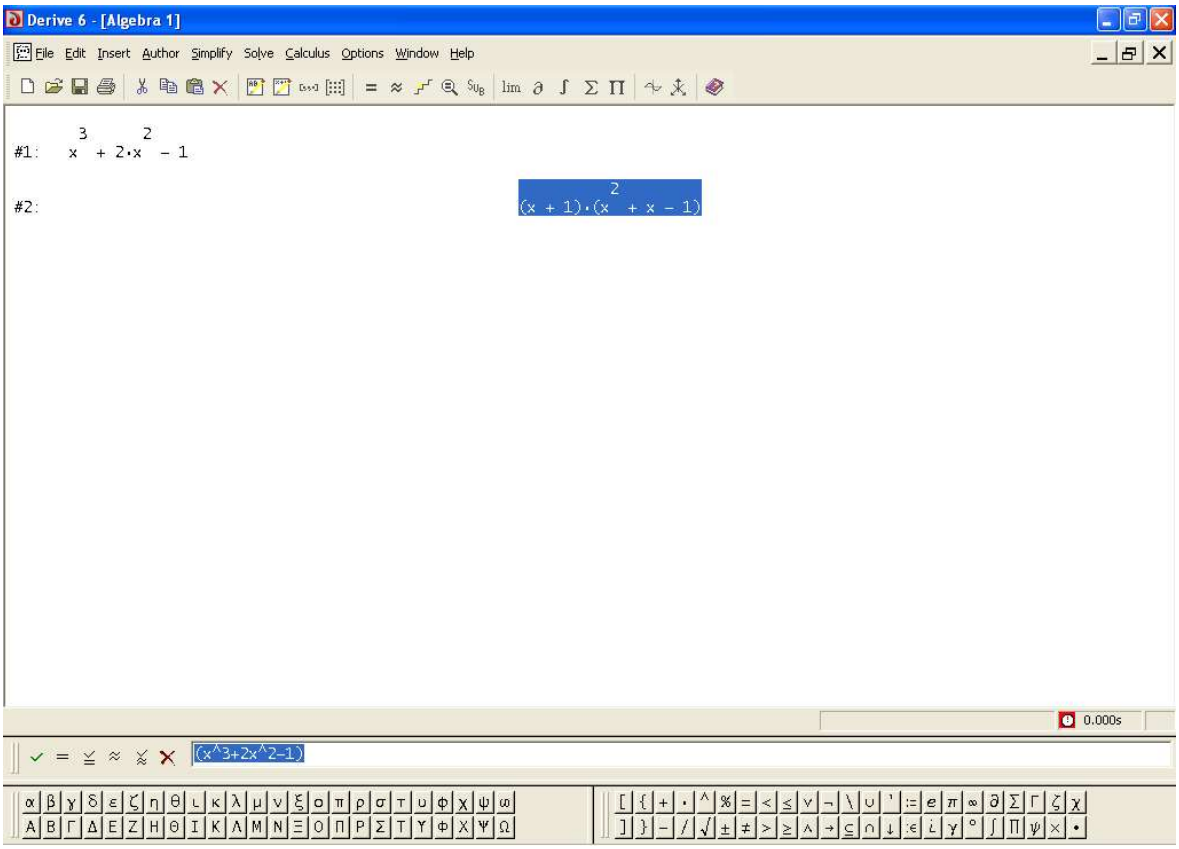


obr.17

Program Derive 6 faktorizoval polynom $f(x) = (x^2 - 1)$ na tyto členy $(x + 1)(x - 1)$, tudíž i jak je patrné z obrázku, zadaný polynom f(x) je reducibilní, tedy rozložitelný.

Příklad 2

Je zadaný polynom $f(x) = x^3 - 2x^2 - 1$ reducibilní nebo ireducibilní?

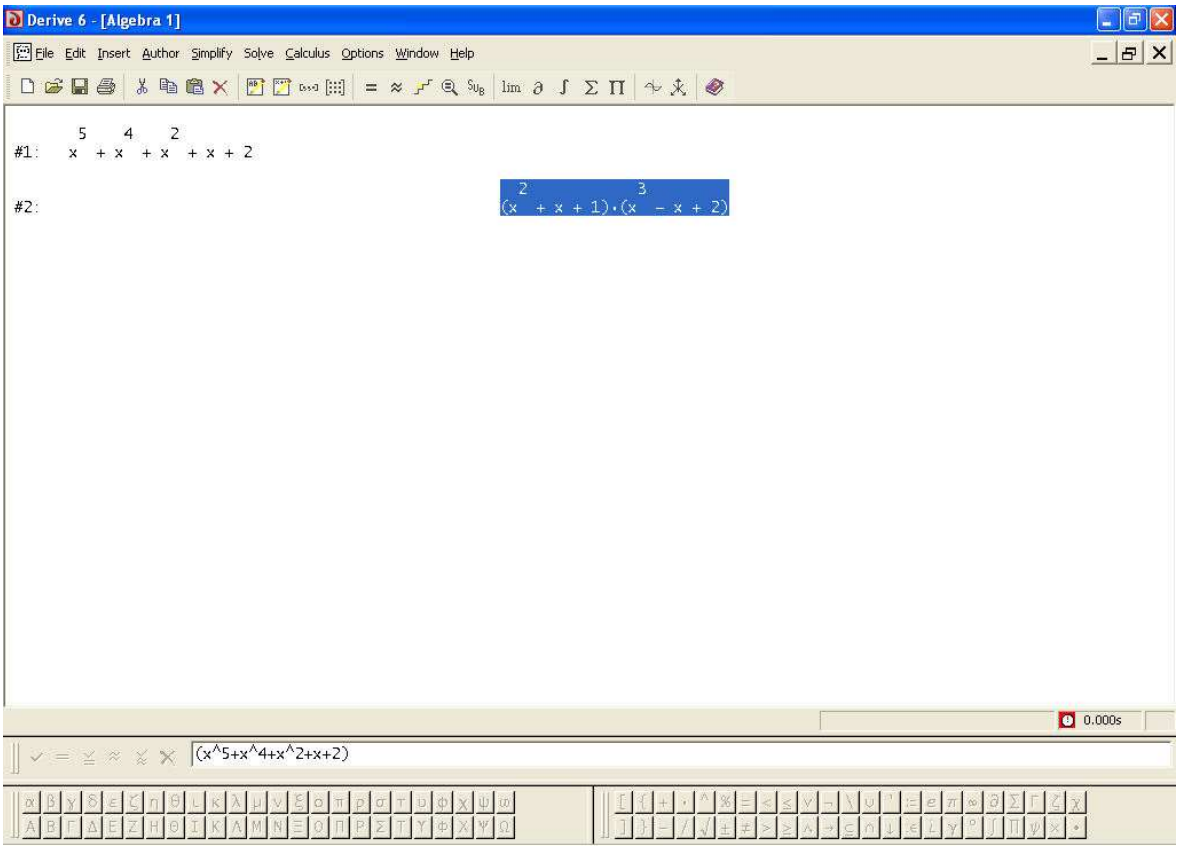


obr.18

Zadaný polynom f(x) je rozložen na členy $(x + 1) \cdot (x^2 + x - 1)$. Opět se tedy jedná o reducibilní polynom.

Příklad 3

Mějme zadaný složitější polynom $f(x) = x^5 + x^4 + x^2 + x + 2$. Rozhodněte, zda se jedná o reducibilní či ireducibilní polynom.

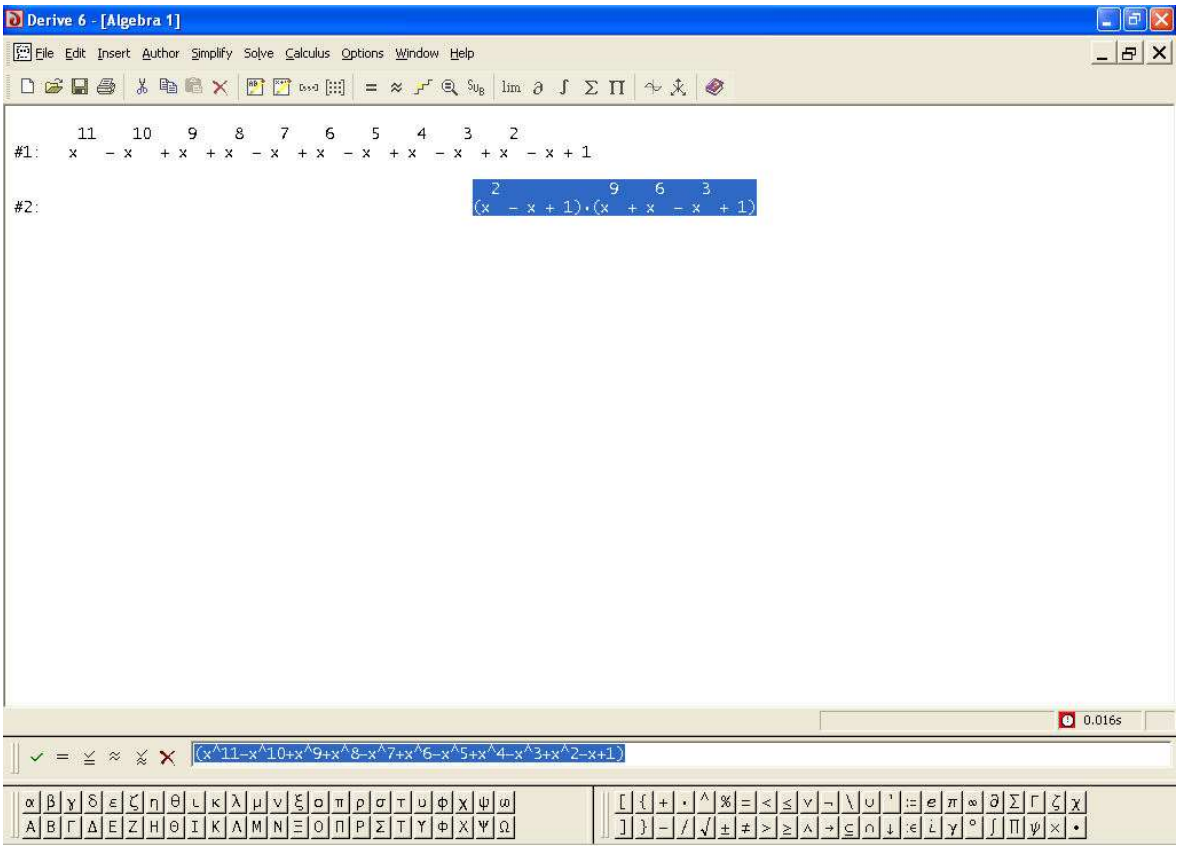


obr.19

Jak už kalkulátor TI - 92 Plus vyřešil totožný příklad, že tento polynom je reducibilní, tak i program Derive 6 zjistil totéž. Polynom byl rozložen na tyto členy $(x^2 + x + 1) \cdot (x^3 - x + 2)$. Tento příklad je vypočítán podrobně i v následující kapitole.

Příklad 4

Polynom $f(x) = x^{11} - x^{10} + x^9 + x^8 - x^7 + x^6 - x^5 + x^4 - x^3 + x^2 - x + 1$. Je zadaný polynom reducibilní nebo ireducibilní?

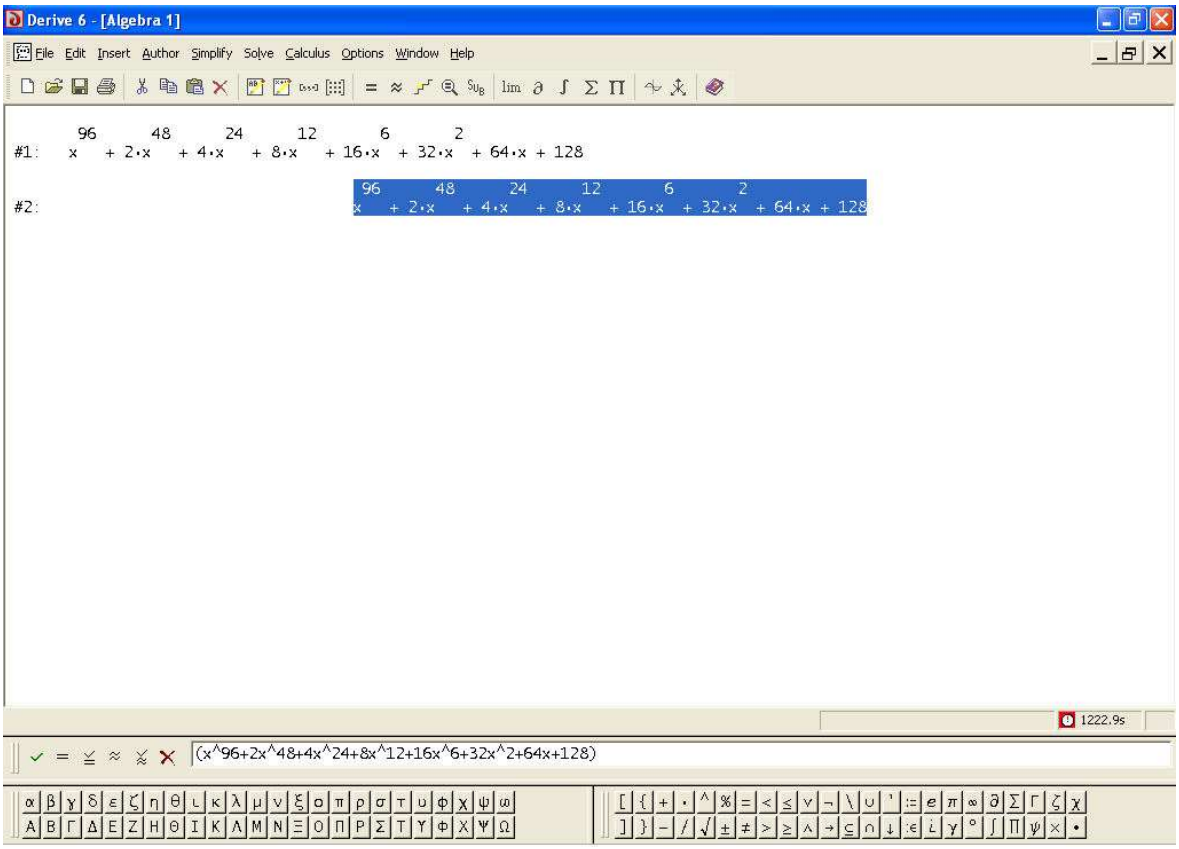


obr.20

Program Derive 6 rozložil zadaný polynom (i když se jedná o složitější) na tyto členy $(x^2 - x + 1) \cdot (x^9 + x^6 - x^3 + 1)$, tudíž je reducibilní.

Příklad 5

Je zadán složitější (náročnější pro program Derive 6) polynom $f(x) = x^{96} + 2x^{48} + 4x^{24} + 8x^{12} + 16x^6 + 32x^2 + 64x + 128$.



obr.21

I přes několikanásobně vyšší stupeň polynomu, než u předchozího příkladu, si s tímto příkladem Derive 6 poradil. Zadaný polynom nerozložil, zůstal v základním tvaru, jedná se tedy o ireducibilní polynom.

Z hlediska výpočetní náročnosti úlohy stojí za povšimnutí čas v pravé dolní části obrázku, za kterou si program Derive 6 dokázal poradit s daným příkladem. Je tedy jasné, čím větší stupeň polynomů, tím déle řešení příkladu v tomto programu trvá.

WolframAlpha

Jedná se o online webové prostředí, které je vytvořeno na základě matematického programu Mathematica. Jelikož je online, můžeme ho využívat při připojení k internetu z jakéhokoliv počítače na webových stránkách www. wolframalpha.com.
Díky tomuto online webovému prostředí WolframAlpha, které je vybaveno sofistikovanějšími algoritmy pro rozklady polynomů než je Kroneckerův algoritmus, lze zvládnout vyřešit více rozsáhlejší a náročnější příklady než pomocí matematických

pomůcek pracujících na bázi Kroneckerova algoritmu, tj. program Derive či kalkulátor TI - 92 Plus.

Při výpočtu jiných matematických příkladů např. integrace a derivace, je nevýhodné, že WolframAlpha zobrazí jen výsledek, ale ne celý postup. Pouze při zaplacení plné verze lze zobrazit celý postup i s výsledkem. Pro faktorizování polynomu stačí zadat do příkazového řádku po zobrazení výše uvedené webové stránky příkaz *„factor“* a zadaný polynom, poté stisknout tlačítko enter a čekat na vygenerování výsledku. Poté můžeme říci, zda je polynom reducibilní nebo ireducibilní. Tento postup lze vidět v následujících příkladech seřazené od polynomů s nižším stupněm po vyšší.

Příklad 1

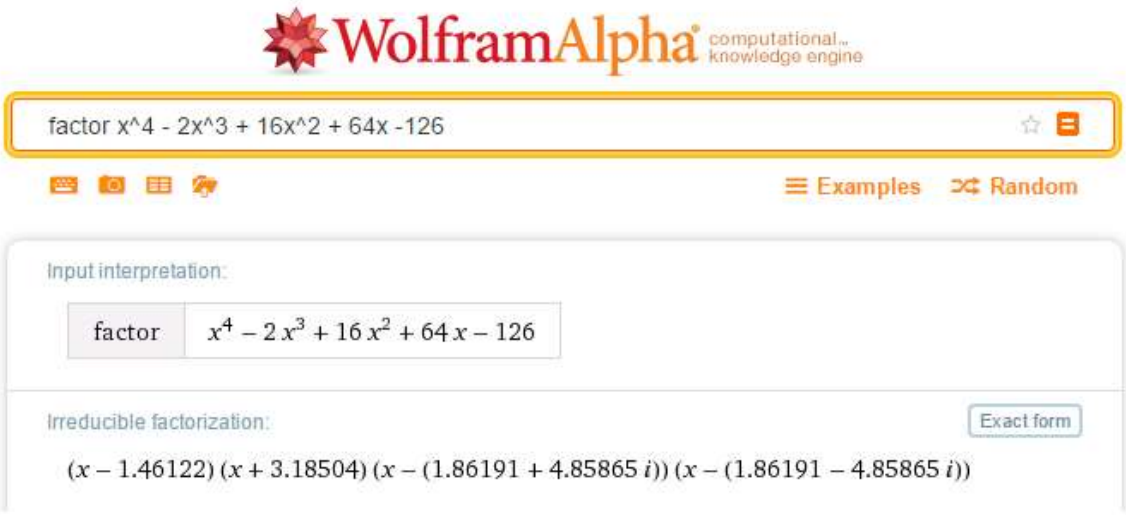
Je zadán polynom $f(x) = x^2 - 1$. Rozhodněte, zda je reducibilní či ireducibilní.

obr.22

Jak je patrné z obrázku, Wolframalpha faktorizoval zadaný polynom a rozložil ho na členy $(x - 1) \cdot (x + 1)$, tudíž můžeme říci, že polynom je reducibilní.

Příklad 2

Mějme zadaný polynom $f(x) = x^4 - 2x^3 + 16x^2 + 64x - 126$. Je zadaný polynom reducibilní nebo ireducibilní?

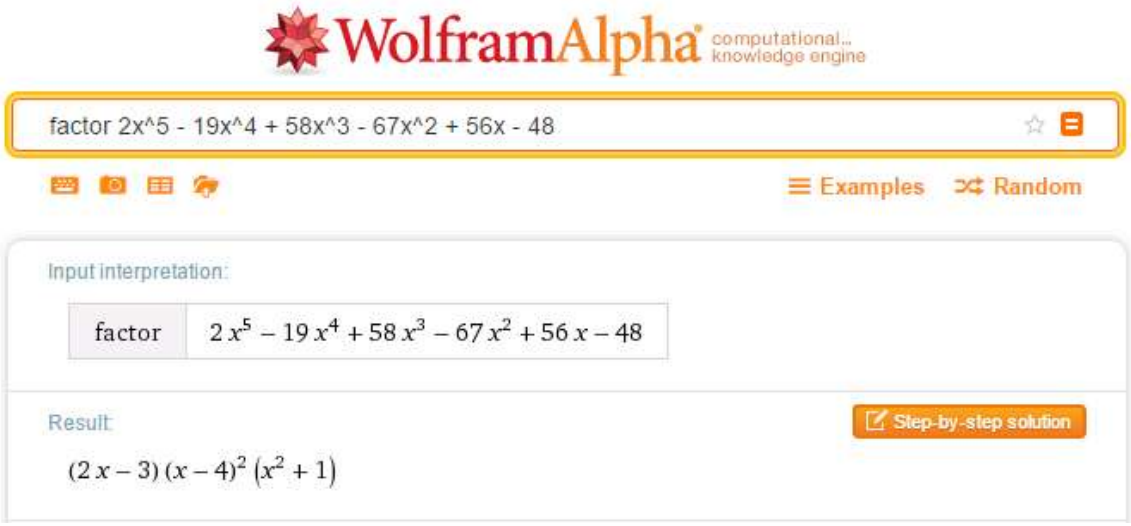


obr.23

WolframAlpha zde vyexportoval typově odlišný výsledek než u předchozího příkladu. Absolutní členy v rozložených členech výsledného mnohočlenu jsou desetinná čísla, tudíž se nenacházíme v Z[x]. Potom je jasné, že zadaný polynom f(x) je ireducibilní, tedy nerozložitelný.

Příklad 3

Mějme zadaný polynom f(x) = $2x^5 - 19x^4 + 58x^3 - 67x^2 + 56x - 48$. Rozhodněte, zda je polynom reducibilní či ireducibilní.

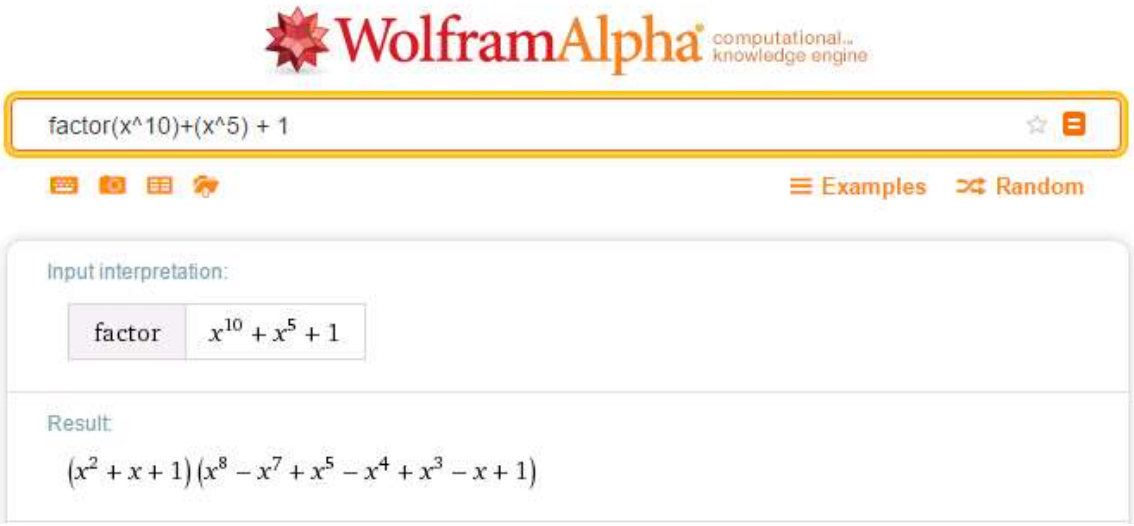


obr.24

Jak je na první pohled zřejmé, tak zadaný polynom byl prostředím WolframAlpha rozložen na tři členy tj. $(2x - 3) \cdot (x - 4)^2 \cdot (x^2 + 1)$, poté můžeme říci, že polynom je reducibilní.

Příklad 4

Je zadán polynom $f(x) = x^{10} + x^5 + 1$. Určete, je-li polynom reducibilní či ireducibilní.

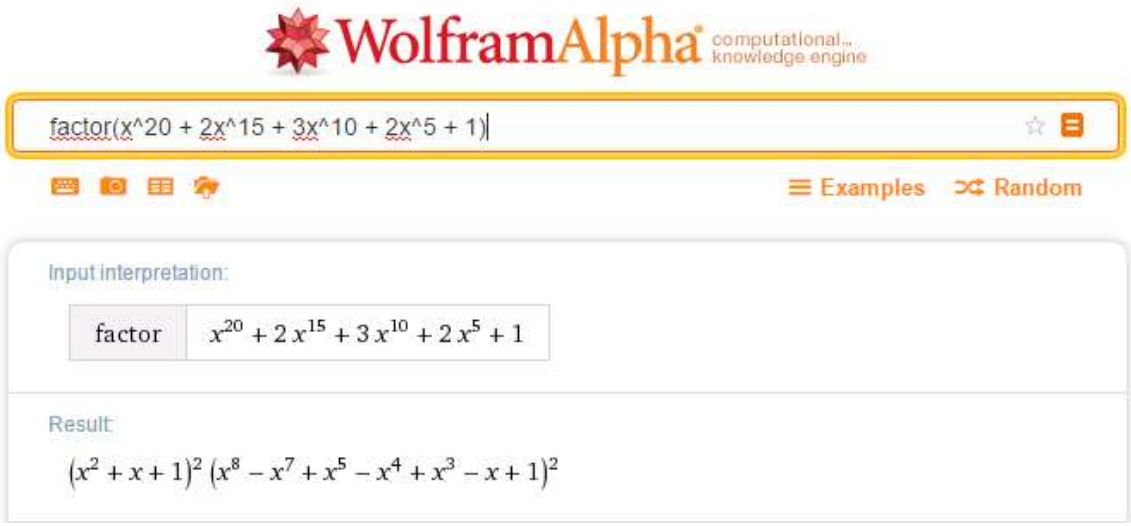


obr.25

Z obrázku je patrné, že WolframAlpha po faktorizaci zadaného polynomu f(x) ho rozložil na dva členy $(x^2 + x + 1) \cdot (x^8 - x^7 + x^5 - x^4 + x^3 - x + 1)$. Z toho tedy můžeme usoudit, že zadaný polynom je reducibilní neboli rozložitelný.

Příklad 5

Je zadán polynom $f(x) = x^{20} + 2x^{15} + 3x^{10} + 2x^5 + 1$. Rozhodněte o reducibilitě nebo ireducibilitě zadaného polynomu.

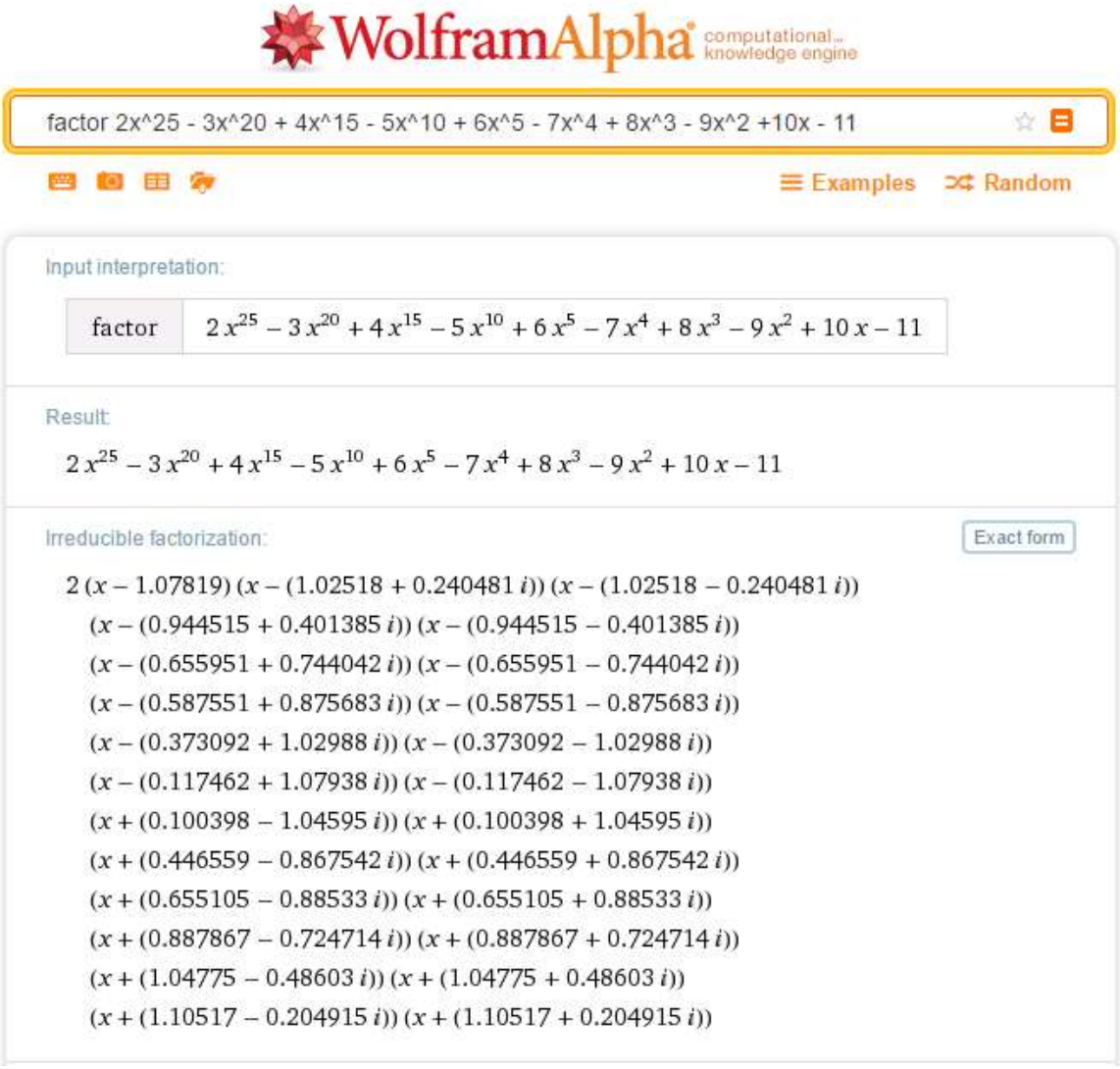


obr.26

WolframAlpha zadaný polynom po faktorizaci rozložil na tyto dva členy $(x^2 + x + 1)^2 \cdot (x^8 - x^7 + x^5 - x^4 + x^3 - x + 1)^2$. Tudíž tedy můžeme říci, že zadaný polynom je reducibilní.

Příklad 6

Mějme zadaný polynom $f(x) = 2x^{25} - 3x^{20} + 4x^{15} - 5x^{10} + 6x^5 - 7x^4 + 8x^3 - 9x^2 + 10x - 11$. Zjistěte, zda je zadaný polynom reducibilní či ireducibilní.



obr.27

Z obrázku je patrné, že polynom je ireducibilní, obdobný rozklad pro faktorizaci jako u příkladu číslo 2, tj. absolutní členy rozložených členů jsou desetinná čísla, tudíž se nenacházíme v Z[x]. Ale také lze zjistit ireducibilitu polynomu po faktorizaci ve WolframAlpha, že nám vygeneruje výsledek stejný jako zadaný polynom.

Řešené příklady

Příklad 1

Zjistěte v Z[x], zda je polynom $f(x) = x^3 + x^2 + x + 1$ reducibilní či ireducibilní.

1. Stupeň polynomu f(x) tj. st f(x) = 3. Mnohočlen g(x) má stupeň nejvýše st g(x) = s = $[\frac{3}{2}] = 1$ a díky tomu lze psát g(x) = ax + b

2. Pro výpočet s + 1 funkčních hodnot mějme x = 0 a 1 (lze zvolit i jiná celá čísla jako hodnoty proměnné x), a tím získáme celočíselné funkční hodnoty *f(0)* = 1 a *f(1)* = 4.

3. Poté lze utvořit množiny všech celočíselných dělitelů čísel *f(0)* = 1 a *f(1)* = 4.
   $D_{f(0)} = \{1, -1\}$;
   $D_{f(1)} = \{1, -1, 2, -2, 4, -4\}$.

4. V tomto bodě jsou ilustrovány jen některé kombinace hodnot *g(0)* a *g(1)*, jelikož by bylo nutné spočítat 12 kombinací, což je velmi zdlouhavé.

   a) Pro každou s + 1-tici čísel $g(0) \in D_{f(0)}$ a $g(1) \in D_{f(1)}$ nalezneme takový (interpolační) polynom *g(x)*, který nabývá v bodech x = 0 a 1 předepsaných hodnot *g(0)* = 1 a *g(1)* = 1. K nalezení Newtonova interpolačního polynomu je důležité sestavit „schéma rozdílu“, do kterého dosadíme hodnoty *g(0)* a *g(1)*,a které vypadá takto:

   1
   0
   1

   Poté zde dostáváme koeficienty:

   $\alpha_0 = \frac{1}{0!} = 1$

   $\alpha_1 = \frac{0}{1!} = 0$

   Tudíž předepsaného tvaru $g(x) = \alpha_0 + \alpha_1(x - a_0) + \alpha_2(x - a_0)(x - a_1) + \ldots + \alpha_s(x - a_0)\ldots(x - a_{s-1})$ dostáváme:

   $g(x) = 1 + 0(x - 0) = 1$.

   Zde je patrné, že je nutné si zvolit jiné vhodné g(0) a g(1), abychom mohli říci, zda polynom f(x) je reducibilní či ireducibilní (viz. krok b)).

b) Mějme interpolační polynomy *g(0)* = 1 a *g(1)* = 4, poté „schéma rozdílu“ bude vypadat následovně:

1

3

4

Následně mějme koeficienty

$\alpha_0 = \frac{1}{0!} = 1$

$\alpha_1 = \frac{3}{1!} = 3$

Z čehož plyne, že *g(x)* = 3x + 1.

Tento polynom g(x) má stupeň st *g(x)* = 1 = s, a je z oboru Z[x].

Nyní rovnou provedeme dělení polynomu g(x) se zadaným polynom f(x).

$(x^3 + x^2 + x + 1)/(3x + 1) = \frac{1}{3}x^2 + \ldots$

$- x^3 - (x^2/3)$ _____

.

.

Polynom g(x) = 3*x* + 1 nemůže být dělitelem, neboť výsledek při dělení má vedoucí člen $\frac{1}{3}x^2$ a nepatří tedy do *Z*[*x*], z toho plyne, že na posledním kroku Kroneckerova algoritmu v tomto případě vůbec nezáleží.

Tudíž budeme pokračovat v následujícím kroku 4c) a zvolíme si vhodné hodnoty *g(0)* a *g(1)*, a sestavím opět „schéma rozdílu“, aby byl výstupem tohoto algoritmu reducibilní polynom.

c) Dále vybíráme jinou kombinaci interpolačních polynomů např. *g(0)* = - 1 a *g(1)* = 4

- 1

3

4

=> $\alpha_0 = \frac{-1}{0!} = -1$

=> $\alpha_1 = \frac{3}{1!} = 3$

Tudíž polynom *g(x)* = 3x - 1.

Polynom *g(x)* je opět stupně st *g(x)* = 1 = s, a je z oboru Z[x].

Opět rovnou provedeme dělení polynomu g(x) se zadaným polynom f(x).

$(x^3 + x^2 + x + 1)/(3x - 1) = \frac{1}{3}x^2$ -...

$- x^3 + (x^2/3)$ _____

.

.

Výsledný polynom g(x) = 3*x* - 1 nemůže opět být dělitelem, neboť výsledek při dělení má vedoucí člen $\frac{1}{3}x^2$ a nepatří tedy do *Z*[*x*], z toho plyne, že na posledním kroku Kroneckerova algoritmu v tomto případě vůbec nezáleží.
Tudíž budeme pokračovat v následujícím kroku 4d), zvolíme si opět vhodné hodnoty *g(0)* a *g(1)* a sestavíme opět „schéma rozdílu“, aby byl výstupem tohoto algoritmu reducibilní polynom.

d) Opět si zvolíme další kombinaci g(0) = 1 a g(1) = 2

1

1

2

=> $\alpha_0 = \frac{1}{0!} = 1$

=> $\alpha_1 = \frac{1}{1!} = 1$

Z čehož mějme více nadějný polynom g(x) = x + 1. Poté následně pokračujme k bodu 5 a budeme opět hledat daný zbytek pro určení i/reducibility polynomu f(x) tj. g(x) dělí f(x).

5. Zde je znázorněn postup hledání nulového zbytku u kombinace *g(0)* = 1 a *g(1)* = 2 pro splnění podmínky a pro ukončení tohoto algoritmu tj. polynom *g(x)* dělí polynom *f(x)*.

Polynom *g(x)* = x + 1 je opět stupně st *g(x)* = 1 = s, a je z oboru Z[x], ale po vydělení mnohočlenu *f(x)* nedostaneme nulový zbytek.

$(x^3 + x^2 + x + 1)/x + 1 = x^2 + 1$

$- x^3 - x^2$_____

$x + 1$

$- x + 1$_____

0 => nulový zbytek

Vyšel nám nulový zbytek, tak lze říci, že *g(x)* dělí *f*(x), což znamená, že polynom f(x) je reducibilní a algoritmus tím končí.

Příklad 2

Mějme zadaný polynom $f(x) = x^3 - x^2 + x - 1$ v Z[x]. Je polynom f(x) ireducibilní či ireducibilní?

1. Dle prvního bodu Kroneckerova algoritmu platí, že n = st *f(x)* = 3 a s = $[\frac{3}{2}] = 1$. Poté je jasné, že polynom g(x) = ax + b, tj. nanejvýše lineární polynom.
2. Zvolíme si hodnotu nezávisle proměnné x, kterou následně dosadíme do polynomu f(x), což v tomto případě bude *f(0)* = - 1 a *f(1)* = 0. Jelikož f(1) = 0, tak je jasné, že 1 bude jedním z kořenů a dále by pak byla $D_{f(1)}$ nekonečná, což je v rozporu s podmínkou Kroneckerova algoritmu.

Polynom je tedy reducibilní, jelikož jsme ve druhém kroku objevili jeden z kořenů (x - 1), a po vydělení polynomu f(x) tímto mnohočlenem nám vyjde další mnohočlen $(x^2 + 1)$. Tudíž rozklad polynomu f(x) je $(x - 1) \cdot (x^2 + 1)$. Můžeme tedy říci, že polynom f(x) je rozložitelný, tedy reducibilní. Tímto algoritmus končí.

Příklad 3

Mějme v Z[x] zadaný polynom *f(x)* = $x^6 - 2x^5 - 5x^4 + 7x^3 - 7x^2 + 4x + 2$. Rozhodněte, zdali je polynom reducibilní či ireducibilní.

1. Stupeň polynomu n = st f(x) = 6, tudíž s = 3. Následně je patrné, že $g(x) = ax^3 + bx^2 + cx + + d$.

2. Poté si zvolíme hodnotu nezávisle proměnné x, kterou následně dosadíme do polynomu f(x). Zde bude vhodné opět zvolit k = 0, 1 a 2. Mějme tedy f(0) = 2, f(1) = 0, f(2) = -42 a f(3) = -22.

3. Dále utvoříme množiny všech celočíselných dělitelů čísel f(0) = 2, f(1) = 0, f(2) = -42 a f(3) = -22.

   $D_{f(0)}$ = {-1, 1, -2, 2};

   $D_{f(1)}$ = nekonečná množina;

   $D_{f(2)}$ = {-1, 1, -2, 2, -3, 3, -6, 6, -7, 7, -14, 14, -28, 28, -42, 42};

   $D_{f(0)}$ = {-1, 1, -2, 2, -11, 11, -22, 22}.

Množina všech celočíselných dělitelů $D_{f(1)}$ je nekonečná, což je v rozporu s podmínkou Kroneckerova algoritmu, tudíž známe jeden z kořenů, který je tedy (x - 1), a po vydělení polynomu f(x) tímto mnohočlenem nám vyjde další mnohočlen ($x^5 - x^4 - 6x^3 + x^2 - 6x - 2$). Tudíž rozklad polynomu f(x) je $(x - 1) \cdot (x^5 - x^4 - 6x^3 + x^2 - 6x - 2)$ a můžeme říci, že polynom f(x) je rozložitelný, tedy reducibilní. Tímto algoritmus končí.

Příklad 4

Zjistěte v Z[x], zda je polynom *f(x)* = $x^5 + x^4 + x^2 + x + 2$ reducibilní či ireducibilní.

1. Nejprve nalezneme stupeň polynomu tj. s = $[\frac{5}{2}]$ = 2, jelikož n = st *f(x)* = 5. Díky tomu zjištění víme, že polynom g(x) = $ax^2 + bx + c$.

2. Nyní si hodnotu nezávisle proměnné x, kterou následně dosadíme do polynomu f(x). Zde bude vhodné opět zvolit k = 0, 1, 2. Mějme tedy f(0) = 2, f(1) = 6 a f(2) = 56

3. Následně utvoříme množiny všech celočíselných dělitelů čísel f(0) = 2, f(1) = 6 a f(2) = 56.

   $D_{f(0)}$ = {-1, 1, -2, 2};

   $D_{f(1)}$ = {-1, 1, -2, 2, -3, 3, -6, 6}

   $D_{f(2)}$ = {-1, 1, -2, 2, -4, 4, -7, 7, -8, 8, -14, 14, -28, 28, -56, 56}

4. V tomto bodě jsou ilustrovány jen některé kombinace hodnot *g(0)* a *g(1)* a *g(2)*, jelikož bychom museli počítat celkem 512 mnohočlenů, což je velmi zdlouhavé. Jako kontrolu zde využijeme kalkulátor TI - 92 Plus a program Derive 6. Výše

zadaný polynom f(x) = $x^5 + x^4 + x^2 + x + 2$ již je ve vzorových příkladech ke kalkulátoru TI - 92 Plus vyřešen (viz obr.8) a také v programu Derive 6 (viz obr. 19). U poslední uvedené kombinace bude splněna podmínka tohoto bodu Kroneckerova algoritmu. tj. polynom *g(x)* dělí polynom *f(x)*, což na konci můžeme poté prohlásit, že polynom f(x) je reducibilní v Z[x].

a) Zde si zvolíme g(0) = 1, g(1) = -3 a g(2) = -14. Poté vneseme tyto hodnoty do „schématu rozdílu“:

1			
	-4		
-3		-7	
	-11		
-14			

Z tohoto schématu zjistíme $\alpha_{0,1,2}$:

$\alpha_0 = \frac{1}{0!} = 1$

$\alpha_1 = \frac{-4}{1!} = -4$

$\alpha_2 = \frac{-7}{2!} = -\frac{7}{2}$

Tudíž máme g(x) = 1 - 4(x- 0) - $\frac{7}{2}$ (x - 0)(x - 1) = - $\frac{7}{2}x^2$ - $\frac{1}{2}$x +1.

Tento výsledný polynom si lze ověřit také pomocí třech rovnic o třech neznámých, zda se jedná opravdu o neceločíselné koeficienty a, b, c ze zjištěného polynomu g(x) = $ax^2 + bx + c$ z prvního kroku.

Mějme tedy:

c = 1

a + b + c = - 3 => a + b = - 4 => b = - 4 - a

4a + 2b + c = - 14 => 4a + 2b = - 15

4a + 2(-4 - a) = -15 => a = - $\frac{7}{2}$ => b = - $\frac{1}{2}$

Po dosazení koeficientů a, b, c nám vychází stejný polynom g(x) = - $\frac{7}{2}x^2$ - $\frac{1}{2}$x +1.

Jelikož ale hledáme polynom s celočíselnými koeficienty, tak tato kombinace zvolených dělitelů je v rozporu s podmínkou tohoto kroku. Poté je zapotřebí se vrátit ke kroku 3 a zvolit novou kombinaci dělitelů pro zjištění reducibility nebo ireducibility polynomů.

b) Další zvolenou kombinací je g(0) = 1, g(1) = -3 a g(2) = 7. Nyní sestavíme „schéma rozdílu“:

1		
	-4	
-3		0
	4	
7		

Poté dostáváme:

$\alpha_0 = \frac{1}{0!} = 1$

$\alpha_1 = \frac{-4}{1!} = -4$

$\alpha_2 = \frac{0}{2!} = 0$

Mějme tedy polynom g(x) = 1 - 4(x- 0) + 0(x - 0)(x - 1) = -4x +1

Zde si ověřovat koeficienty a, b, c nemusíme, jelikož už nám celočíselně vyšly. Díky tomu lze ihned dělit zadaný polynom f(x) polynomem g(x) = -4x + 1.

$x^5 + x^4 + x^2 + x + 2/(-4x + 1) = -\frac{1}{4}x^4 - \ldots$

$-x^5 - x^4/4$

.

.

Výsledný polynom g(x) = -4*x* + 1 nemůže být dělitelem, neboť výsledek při dělení má vedoucí člen $\frac{1}{3}x^2$ a nepatří tedy do *Z*[*x*], z toho plyne, že na posledním kroku Kroneckerova algoritmu v tomto případě vůbec nezáleží.

Tudíž budeme pokračovat v následujícím kroku 4c) a zvolíme si opět vhodné hodnoty *g(0)* a *g(1)*, a opět sestavíme „schéma rozdílu“, aby byl výstupem tohoto algoritmu reducibilní polynom.

c) Poslední zvolenou úspěšnou kombinací v tomto příkladu je g(0) = 1, g(1) = 3 a také g(2) = 7. Opět tyto vybrané dělitele znázorníme na „schéma rozdílu“:

1		
	2	
3		2
	4	
7		

Následně dostáváme:

$\alpha_0 = \frac{1}{0!} = 1$

$\alpha_1 = \frac{2}{1!} = 2$

$\alpha_2 = \frac{2}{2!} = 1$

Poté dostaneme polynom $g(x) = 1 + 2(x - 0) + 1(x - 0)(x - 1) = x^2 + x + 1$.

Nyní ještě můžeme, pokud chceme, ověřit koeficienty pomocí třech rovnic o třech neznámých, zdali jsou celočíselné z polynomu $g(x) = ax^2 + bx + c$ z prvního kroku.

$c = 1$

$a + b + c = 3 \quad \Rightarrow a + b = 2 \Rightarrow b = 2 - a$

$4a + 2b + c = 7 \Rightarrow 4a + 2b = 6$

$4a + 2(2 - a) = 6 \qquad \Rightarrow a = 1 \Rightarrow b = 1$

Po dosazení koeficientů a, b, c nám opět vychází stejný polynom $g(x) = x^2 + x + 1$. Poté přejděme k následujícímu kroku zjistit nulový či nenulový zbytek při dělení mnohočlenů.

5. Mějme tedy člen $x^2 + x + 1$ z kroku 4c) a zde je zapotřebí zjistit, zdali polynom g(x) dělí polynom f(x) s nulovým zbytkem.

   $x^5 + x^4 + x^2 + x + 2 / x^2 + x + 1 = x^3 - x + 2$

   $- x^5 - x^4 - x^3$

   $- x^3 + x^2 + x + 2$

   $- x^3 - x^2 - x$

   $2x^2 + 2x + 2$

   $-2x^2 - 2x - 2$

   0 => nulový zbytek

   Jelikož nám vyšel nulový zbytek, můžeme říci, že polynom g(x) dělí polynom f(x) a získali jsme tím rozklad ve tvaru $f(x) = g(x) \cdot h(x)$, kde h(x) je v Z[x]. Tímto jsme příklad vyřešili a algoritmus končí.

Příklad 5

Rozhodněte, zda je polynom $f(x) = x^2 + x + 1$ v Z[x] reducibilní či ireducibilní.

1. Stupeň polynomu n = st f(x) = 2, tudíž s = 1. Poté je patrné, že g(x) = ax + b.
2. Dále si zvolíme hodnotu nezávisle proměnné x, kterou následně dosadíme do polynomu f(x). Zde bude vhodné opět zvolit k = 0 a 1. Mějme tedy f(0) = 1 a f(1) = 3.
3. Následně utvoříme množiny všech celočíselných dělitelů čísel f(0) = 1 a f(1) = 3.
   $D_{f(0)}$ = {-1, 1};
   $D_{f(1)}$ = {-1, 1, -3, 3}
4. Zde si předvedeme všechny kombinace hodnot *g(0)* a *g(1)*, abychom se opravdu přesvědčili, že ani jedna kombinace nesplňuje krok 5 Kroneckerova algoritmus, tj. polynom *g(x)* dělí polynom *f(x)* (viz níže).
   a) Mějme tedy g(0) = 1 a g(1) = 1. Poté „schéma rozdílu“ bude vypadat takto:

   1
   0
   1

   Poté tedy dostaneme:

   $\alpha_0 = \frac{1}{0!} = 1$

   $\alpha_1 = \frac{0}{1!} = 0$

   Tudíž se g(x) = 1, a pokud bychom za g(x) zvolili stejné čísla tj. g(0) = -1 a g(1) = -1, tak dospějeme do podobné situace, že polynom g(x) vyjde konkrétní číslo:

   -1
   0
   -1

   Následně vyjde:

   $\alpha_0 = \frac{-1}{0!} = -1$

   $\alpha_1 = \frac{0}{1!} = 0$

   A opět dostaneme polynom g(x) jako číslo, tj. g(x) = -1.
   Ani jedna z těchto variant není vhodná, jelikož by se zadaný polynom nerozložil na

mnohočleny při dělení konkrétním číslem. Tím pádem musíme zvolit jinou kombinaci g(0) a g(1).

b) Nyní mějme g(0) = 1 a g(1) = -1. Dále sestavíme „schéma rozdílu“ :

1
-2
-1

Koeficienty:

$\alpha_0 = \frac{1}{0!} = 1$

$\alpha_1 = \frac{-2}{1!} = -2$

Z toho plyne, že g(x) = -2x + 1.

Polynom *g(x)* je opět stupně st *g(x)* = 1 = s, a je z oboru Z[x].

Následně provedeme dělení polynomu g(x) se zadaným polynom f(x).

Mějme mnohočlen -2x + 1, kterým vydělíme mnohočlen $x^2 + x + 1$.

$(x^2 + x + 1)/-2x + 1 = -\frac{1}{2}x$ -...

$-x^2 + (x/2)$ _____

.

.

Výsledný polynom g(x) = -2*x* + 1 nemůže být dělitelem, neboť výsledek při dělení má vedoucí člen $-\frac{1}{2}x$ a nepatří tedy do *Z*[*x*], z toho plyne, že na posledním kroku Kroneckerova algoritmu v tomto případě vůbec nezáleží.

Tudíž budeme pokračovat v následujícím kroku 4c) a zvolíme si opět vhodné hodnoty *g(0)* a *g(1)*, a opět sestavíme „schéma rozdílu“, aby byl výstupem tohoto algoritmu reducibilní polynom.

c) Další kombinaci si zvolme g(0) = 1 a g(1) = 3. Poté „schéma rozdílu“ bude vypadat následovně:

1
2
3

Koeficienty:

$\alpha_0 = \frac{1}{0!} = 1$

$\alpha_1 = \frac{2}{1!} = 2$

Tudíž dostaneme g(x) = 2x + 1.

Výsledný polynom *g(x)* je opět stupně st *g(x)* = 1 = s, a je z oboru Z[x].

Opět rovnou provedeme dělení polynomu g(x) se zadaným polynom f(x).

Mějme tentokrát mnohočlen 2x + 1, kterým vydělíme mnohočlen $x^2 + x + 1$.

$(x^2 + x + 1)/2x + 1 = \frac{1}{2}x + \ldots$

$\underline{- x^2 - (x/2)\quad\quad}$

.

.

Výsledný polynom g(x) = 2*x* + 1 nemůže opět být dělitelem, neboť výsledek při dělení má vedoucí člen $\frac{1}{2}x$ a nepatří tedy do *Z*[*x*], z toho plyne, že na posledním kroku Kroneckerova algoritmu v tomto případě vůbec nezáleží.

Tudíž budeme pokračovat v následujícím kroku 4d) a zvolíme si opět vhodné hodnoty *g(0)* a *g(1)*, a opět sestavíme „schéma rozdílu“, aby byl výstupem tohoto algoritmu reducibilní polynom.

d) Poté zkusíme kombinaci g(0) = 1 a g(1) = -3. Následně schéma rozdílu bude mít následující podobu:

1

-4

-3

Koeficienty:

$\alpha_0 = \frac{1}{0!} = 1$

$\alpha_1 = \frac{-4}{1!} = -4$

Z čehož dostaneme, že g(x) = -4x + 1.

Výsledný polynom *g(x)* je opět stupně st *g(x)* = 1 = s, a je z oboru Z[x].

Opět rovnou provedeme dělení polynomu g(x) se zadaným polynom f(x).

Zde mějme mnohočlen $x^2 + x + 1$ vydělíme mnohočlenem -4x + 1.

$(x^2 + x + 1)/-4x + 1 = -\frac{1}{4}x$ -…

$\underline{- x^2 + (x/4)\quad\quad}$

.

.

Výsledný polynom g(x) = -4*x* + 1 nemůže opět být dělitelem, neboť výsledek při dělení má vedoucí člen $-\frac{1}{4}x$ a nepatří tedy do *Z*[*x*], z toho plyne, že na posledním kroku Kroneckerova algoritmu v tomto případě vůbec nezáleží.

Tudíž budeme pokračovat v následujícím kroku 4e) a zvolíme si opět vhodné hodnoty *g(0)* a *g(1)*, a opět sestavíme „schéma rozdílu“, aby byl výstupem tohoto algoritmu reducibilní polynom.

e) Opět mějme jinou kombinaci g(0) = -1 a g(1) = 1. Tudíž „schéma rozdílu“ bude vypadat následovně:

-1

2

1

Koeficienty:

$\alpha_0 = \frac{-1}{0!} = -1$

$\alpha_1 = \frac{2}{1!} = 2$

Z toho plyne, že g(x) = 2x - 1.

Výsledný polynom *g(x)* je opět stupně st *g(x)* = 1 = s, a je z oboru Z[x].

Opět rovnou provedeme dělení polynomu g(x) se zadaným polynom f(x).

Mějme tentokrát mnohočlen 2x - 1, kterým vydělíme mnohočlen $x^2 + x + 1$.

$(x^2 + x + 1)/2x - 1 = \frac{1}{2}x$ +…

$\underline{- x^2 + (x/2)\quad\quad}$

.

.

Výsledný polynom g(x) = 2*x* - 1 nemůže opět být dělitelem, neboť výsledek při dělení má vedoucí člen $\frac{1}{2}x$ a nepatří tedy do *Z*[*x*], z toho plyne, že na posledním kroku Kroneckerova algoritmu v tomto případě vůbec nezáleží.
Tudíž budeme pokračovat v následujícím kroku 4f) a zvolíme si opět vhodné hodnoty *g(0)* a *g(1)*, a opět sestavíme „schéma rozdílu“, aby byl výstupem tohoto algoritmu reducibilní polynom.

f) Další kombinaci si zvolme g(0) = -1 a g(1) = 3. Poté „schéma rozdílu“ bude vypadat takto:

-1
4
3

Koeficienty:

$\alpha_0 = \frac{-1}{0!} = -1$

$\alpha_1 = \frac{4}{1!} = 4$

Tudíž dostaneme g(x) = 4x - 1.

Výsledný polynom *g(x)* je opět stupně st *g(x)* = 1 = s, a je z oboru Z[x].

Opět rovnou provedeme dělení polynomu g(x) se zadaným polynom f(x).

Mějme mnohočlen 4x - 1, kterým vydělíme mnohočlen $x^2 + x + 1$.

$(x^2 + x + 1)/4x - 1 = \frac{1}{4}x + \ldots$

$\underline{- x^2 + (x/4) \quad\quad}$

.

.

Výsledný polynom g(x) = 4*x* - 1 nemůže opět být dělitelem, neboť výsledek při dělení má vedoucí člen $\frac{1}{4}x$ a nepatří tedy do *Z*[*x*], z toho plyne, že na posledním kroku Kroneckerova algoritmu v tomto případě vůbec nezáleží.
Tudíž budeme pokračovat v následujícím kroku 4g) a zvolíme si opět vhodné hodnoty *g(0)* a *g(1)*, a opět sestavíme „schéma rozdílu“, aby byl výstupem tohoto algoritmu reducibilní polynom.

g) Poslední kombinaci mějme g(0) = -1 a g(1) = -3. Poté „schéma rozdílu“ bude vypadat:

-1

-2

-3

Koeficienty:

$\alpha_0 = \frac{-1}{0!} = -1$

$\alpha_1 = \frac{-2}{1!} = -2$

Tudíž dostaneme g(x) = -2x - 1.

Výsledný polynom *g(x)* je opět stupně st *g(x)* = 1 = s, a je z oboru Z[x].

Opět rovnou provedeme dělení polynomu g(x) se zadaným polynom f(x).

Mějme mnohočlen -2x - 1, kterým vydělíme mnohočlen $x^2 + x + 1$.

$(x^2 + x + 1)/-2x - 1 = -\frac{1}{2}x\ldots$

$\underline{- x^2 - (x/2)\quad\quad}$

.

.

Výsledný polynom g(x) = -2*x* - 1 nemůže opět být dělitelem, neboť výsledek při dělení má vedoucí člen $-\frac{1}{2}x$ a nepatří tedy do *Z*[*x*], z toho plyne, že na posledním kroku Kroneckerova algoritmu v tomto případě vůbec nezáleží.
Jelikož jsme již vyčerpali všechny možné kombinace g(0) a g(1), nelze si již zvolit další hodnoty *g(0)* a *g(1)*, a opět sestavit „schéma rozdílu“, aby byl výstupem tohoto algoritmu reducibilní polynom.

5. Vyčerpali jsme všechny možné kombinace. Z toho plyne, že polynom g(x) nedělí polynom f(x), tj. polynom f(x) je ireducibilní, a algoritmus končí.

Příklad 6

Zjistěte v Z[x], zda je polynom *f(x)* = $6x^4 - x^3 + 4x^2 - x - 1$ reducibilní či ireducibilní.

1. Stupeň polynomu n = st f(x) = 4, tudíž s = 2. Poté je jasné, že g(x) = $ax^2 + bx + c$.

2. Dále si zvolíme hodnotu nezávisle proměnné x, kterou následně dosadíme do polynomu f(x). Zde bude vhodné opět zvolit k = 0, 1 a 2. Mějme tedy f(0) = -2, f(1) = 6 a f(2) = 100.

3. Následně utvoříme množiny všech celočíselných dělitelů čísel f(0) = -2, f(1) = a f(2) = 100.

   $D_{f(0)}$ = {-1, 1, -2, 2};

   $D_{f(1)}$ = {-1, 1, -2, 2, -3, 3, -6, 6}

   $D_{f(2)}$ = {-1, 1, -2, 2, -4, 4, -5, 5, -10, 10, -20, 20, -25, 25, -50, 50, -100, 100}

4. V tomto bodě je ilustrována jen jedna úspěšná kombinace hodnot *g(0)*, *g(1)* a *g(2)* (=> f(x) je reducibilní), jelikož by bylo nutné vypočítat 4 · 8 · 18 = 576 různých kombinací polynomu g(x), což je značně časově náročné.

   Tudíž g(0) = 1, g(1) = 3 a g(2) = 5, a „schéma rozdílu“ bude vypadat takto:

   1
   2
   3 0
   2
   5

   Poté mějme koeficienty:

   $\alpha_0 = \frac{1}{0!} = 1$

   $\alpha_1 = \frac{2}{1!} = 2$

   $\alpha_2 = \frac{0}{2!} = 0$

   Z toho dostáváme, že g(x) = 1 + 2(x - 0) + 0(x - 0)(x - 1) = 2x + 1. Pokračovat budeme krokem 5 za cílem zjištění, že je polynom f(x) reducibilní, jak už je nepatrně naznačeno v popisu kroku 4.

5. Z předchozího kroku mějme mnohočlen 2x + 1, kterým vydělíme mnohočlen $6x^4 - x^3 + 4x^2 - x - 1$.

   $(6x^4 - x^3 + 4x^2 - x - 1)/(2x + 1) = 3x^3 - 2x^2 + 3x - 2$

   $- 6x^4 - 3x^3$

   $- 4x^3 + 4x^2 - x - 2$

   $4x^3 + 2x^2$

$6x^2 - x - 2$

$\underline{- 6x^2 - 3x}$

$- 4x - 2$

$\underline{4x + 2}$

0 => nulový zbytek => g(x) dělí f(x) => f(x) je reducibilní => algoritmus končí.

Příklad 7

Rozhodněte, zdali zadaný polynom $f(x) = x^{10} - 2x^9 + 5x^8 - 4x^7 + 4x^6 + x^4 - 2x^3 + 5x^2 - 4x + 4$ je reducibilní nebo ireducibilní.

1. Stupeň polynomu n = st f(x) = 10, tudíž s = 5. Tudíž je $g(x) = ax^5 + bx^4 + cx^3 + dx^2 + ex + f$
2. Dále si zvolíme hodnotu nezávisle proměnné x, kterou následně dosadíme do polynomu f(x). Zde bude vhodné si zvolit k = -2, -1, 0, 1, 2, 3. Po dosazení k-hodnot do zadaného polynomu f(x) dostaneme hodnoty f(-2) = 4160, f(-1) = 32, f(0) = 4, f(1) = 8, f(2) = 1040 a f(3) = 46720. Z toho je patrné, že některé hodnoty f(k) nabývají vysokých hodnot.
3. Následně utvoříme množiny všech celočíselných dělitelů čísel f(-2) = 4160, f(-1) = 32, f(0) = 4, f(1) = 8, f(2) = 1040 a f(3) = 46720. Jelikož některé hodnoty f(k) nabývají vysokých hodnot, uvedeme u nich jen počet dělitelů, protože vypisování všech by bylo časově náročné.

   $D_{f(-2)}$ = množina obsahující 56 dělitelů

   $D_{f(-1)}$ = {-1, 1, -2, 2, -4, 4, -8, 8, -16, 16, -32, 32}

   $D_{f(0)}$ = {-1, 1, -2, 2, -4, 4}

   $D_{f(1)}$ = {-1, 1, -2, 2, -4, 4, -8, 8};

   $D_{f(2)}$ = množina obsahující 40 dělitelů

   $D_{f(3)}$ = množina obsahující 64 dělitelů
4. V tomto bodě je opět ilustrována jen jedna úspěšná kombinace hodnot *g(-2)*, *g(-1)*, *g(0)*, *g(1)*, *g(2)* a *g(3)* (=> f(x) je reducibilní), jelikož by bylo nutné vypočítat $56 \cdot 12 \cdot 6 \cdot 8 \cdot 40 \cdot 64 = 82\,575\,360$ různých kombinací polynomu g(x), což je značně časově náročné.

   Tudíž g(-2) = 8, g(-1) = 4, g(0) = 2, g(1) = 2, g(2) = 4 a g(3) = 8 a „schéma rozdílu“

bude vypadat takto:

8								
	-4							
4		2						
	-2		0					
2		2		0				
	0		0		0			
2		2		0				
	2		0					
4		2						
	4							
8								

Poté mějme koeficienty:

$\alpha_0 = \frac{8}{0!} = 8$

$\alpha_1 = \frac{-4}{1!} = -4$

$\alpha_2 = \frac{2}{2!} = 1$

$\alpha_3 = \frac{0}{3!} = 0$

$\alpha_4 = \frac{0}{4!} = 0$

$\alpha_5 = \frac{0}{5!} = 0$

Z toho dostáváme, že $g(x) = x^2 - x + 2$.

5. Z předchozího kroku mějme mnohočlen $x^2 - x + 2$, kterým vydělíme zadaný mnohočlen $f(x) = x^{10} - 2x^9 + 5x^8 - 4x^7 + 4x^6 + x^4 - 2x^3 + 5x^2 - 4x + 4$.

$x^{10} - 2x^9 + 5x^8 - 4x^7 + 4x^6 + x^4 - 2x^3 + 5x^2 - 4x + 4 / x^2 - x + 2 = x^8 - x^7 + 2x^6 + x^2 - x + 2$

$- x^{10} + x^9 - 2x^8$

$- x^9 + 3x^8 - 4x^7 + 4x^6 + x^4 - 2x^3 + 5x^2 - 4x + 4$

$x^9 - x^8 + 2x^7$

$2x^8 - 2x^7 + 4x^6 + x^4 - 2x^3 + 5x^2 - 4x + 4$

$- 2x^8 + 2x^7 - 4x^6$

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

$- x^4 + x^3 - 2x^2$

$- x^3 + 3x^2 - 4x + 4$

$\underline{x^3 - x^2 + 2x}$

$2x^2 - 2x + 4$

$\underline{- 2x^2 + 2x - 4}$

0 => nulový zbytek => g(x) dělí f(x) => f(x) je reducibilní => algoritmus končí.

Na tomto příkladu je ilustrována časová náročnost procesu výpočtu pomocí Kroneckerova algoritmu. Jak už je uvedeno v kroku 4 tohoto příkladu, množiny dělitelů mají postupně 56, 12, 6, 8, 40 a 64 dělitelů, což dává dohromady 82 575 360 možných kombinací, které by musel teoreticky Kroneckerův algoritmus projít. Pokud by každé kombinaci bylo věnováno 10 ms výpočetního času, zabralo by to celkem 229,376 hodin, tj. 9,557 dne. Tudíž je jasné, jak neefektivní může Kroneckerův algoritmus být, i když pro pochopení je jednoduchý.

Závěr

Touto prací je vysvětlen Kroneckerův algoritmus a všechny důležité aspekty, které se jej týkají. V úvodu je podrobně popsán algebraický pojem polynom, kde jsou znázorněny vlastnosti polynomů, jejich rozdělení a práce s nimi. Tento pojem je pro práci nesmírně důležitý, jelikož Kroneckerův algoritmus pracuje právě s polynomy s celočíselnými koeficienty v oboru Z[x].

Další kapitola se zabývá historickým vývojem podobných algoritmů či kritérii zabývajícími se faktorizací polynomů podobného typu jako Kroneckerův algoritmus. Zde je vidět, jakým způsobem se matematika, spíše tedy algebra, vyvíjela od dob Babyloňanů, tj. 1900 - 1600 př. n. l., do současnosti. U některých z kritérií a algoritmů je uveden názorný stručný příklad pro jasné pochopení.

Následně je popsán také život zakladatele tohoto algoritmu, který je právě podle něho pojmenován, jedná se tedy o Leopolda Kroneckera - jaké vyznával náboženství během života, z jaké rodiny pocházel. Dále jsou v této kapitole zmíněny jeho středoškolské a vysokoškolské studie, dále způsob, jak získal matematické uznání a prestiž mezi ostatními vyhlášenými matematikami díky svým matematickým objevům a postupům.

Poté následuje teoretický základ Kroneckerova algoritmu, u kterého je popsán krok po kroku, jak probíhá, abychom na konci tohoto algoritmu, tedy po vyřešení všech kombinací dělitelů polynomů f(x), kde x = 0, 1,…,s, mohli říci, zda-li zadaný polynom je reducibilní (rozložitelný) či ireducibilní (nerozložitelný), polynom $f(x)$ lze zapsat jako součin dvou polynomů nižších stupňů. Celý postup tohoto algoritmu je vysvětlen ve vzorovém příkladu.

Dále je ilustrováno praktické využití tohoto algoritmu na kalkulátoru TI - 92 Plus a také na programu Derive 6, který jako kalkulátor TI - 92 plus pracuje na bázi Kroneckerova algoritmu. Dále také lze využít webové prostředí WolframAlpha, které nepracuje na bázi Kroneckerova algoritmu, pro srovnání některých příkladů, které jsou řešené v tomto prostředí. Tyto matematické pomůcky jsou velmi praktické. Doba faktorizování daného mnohočlenu sice závisí na složitosti příkladu, ale u mnohočlenů nejvýše do cca 10. stupně dokáží vyřešit v rychlém čase zadaný příklad. Poté s náročností příkladu roste doba jeho

vyřešení. Usnadní nám tedy sáhodlouhé rozkládání mnohočlenu na faktory u vyšších stupňů, ale také i u mnohočlenů, pro které jsou známé vzorce pro rozklad, ale my si je nepamatujeme.

A na konci této práce jsou v poslední kapitole řešeny příklady krok po kroku a aplikované různé možné varianty průběhu Kroneckerova algoritmu, zdali se jedná o reducibilní nebo ireducibilní polynom, poté zda se při výběru polynomu f(x), kde x = 0, 1,…,s, bude hodnota f(x) = 0, tudíž poté x je kořenem daného mnohočlenu, a také se poruší podmínka tohoto algoritmu, že žádná z množin dělitelů $D_{f(x)}$ nesmí být nekonečná, což u tohoto příkladu nastává.

Resumé

The Kronecker´s algorithm is used for factorization of polynomials in the domain of whole numbers and thanks to that we can find out if there is reserved polynomial reducible or irreducible. The author of this algorithm is Leopold Kronecker, who is a German mathematician. For the factorization of polynomials there is possible to use the mathematical aids, which work on the basis of the Kronecker´s algorithm (for example a calculator Ti-92 PLUS, Derive 6 from the company Texas Instrument, Inc.). These aids speed up the factorization of polynomials and we can easily get the reducible or irreducible polynomial.

Seznam použité literatury a webových zdrojů

[1] HORA, Jaroslav. Kroneckerův algoritmus. *Rozhledy matematicko-fyzikální*. 1992, roč. 69, č. 5, s. 199-202.

[2] GATHEN, Joachim von zur a Jürgen GERHARD. *Modern Computer Algebra*. 2nd ed. Cambridge: Cambridge University Press, 2003, xiii, 785 s. ISBN 05-218-2646-2.

[3] DAVENPORT, James Harold, Y. SIRET a E TOURNIER. Computer algebra: systems and algorithms for algebraic computation. San Diego: Academic Press, 1988, xix, 267 s. ISBN 01-220-4230-1.

[4] LISKA, Richard a kol. *Algoritmy pro algebraické výpočty* [online]. 1998. Dostupné z: http://www-troja.fjfi.cvut.cz/~liska/poalg/node7.html.

[5] HONZÍK, Lukáš. *Některé metoda faktorizace polynomů*. Plzeň, 2007. Diplomová práce. ZČU v Plzni. Vedoucí práce doc. RNDr. Jaroslav Hora, CSc.

[6] Factorization of polynomials. *Wikipedia: The Free Encyclopedia* [online]. [cit. 2016-04-01].

Dostupné z: https://en.wikipedia.org/wiki/Factorization_of_polynomials

[7] Leopold Kronecker. MacTutor History of Mathematics, [online]. [cit. 2016-04-01]. Dostupné z: http://www-gap.dcs.st-and.ac.uk/history/Biographies/Kronecker.html

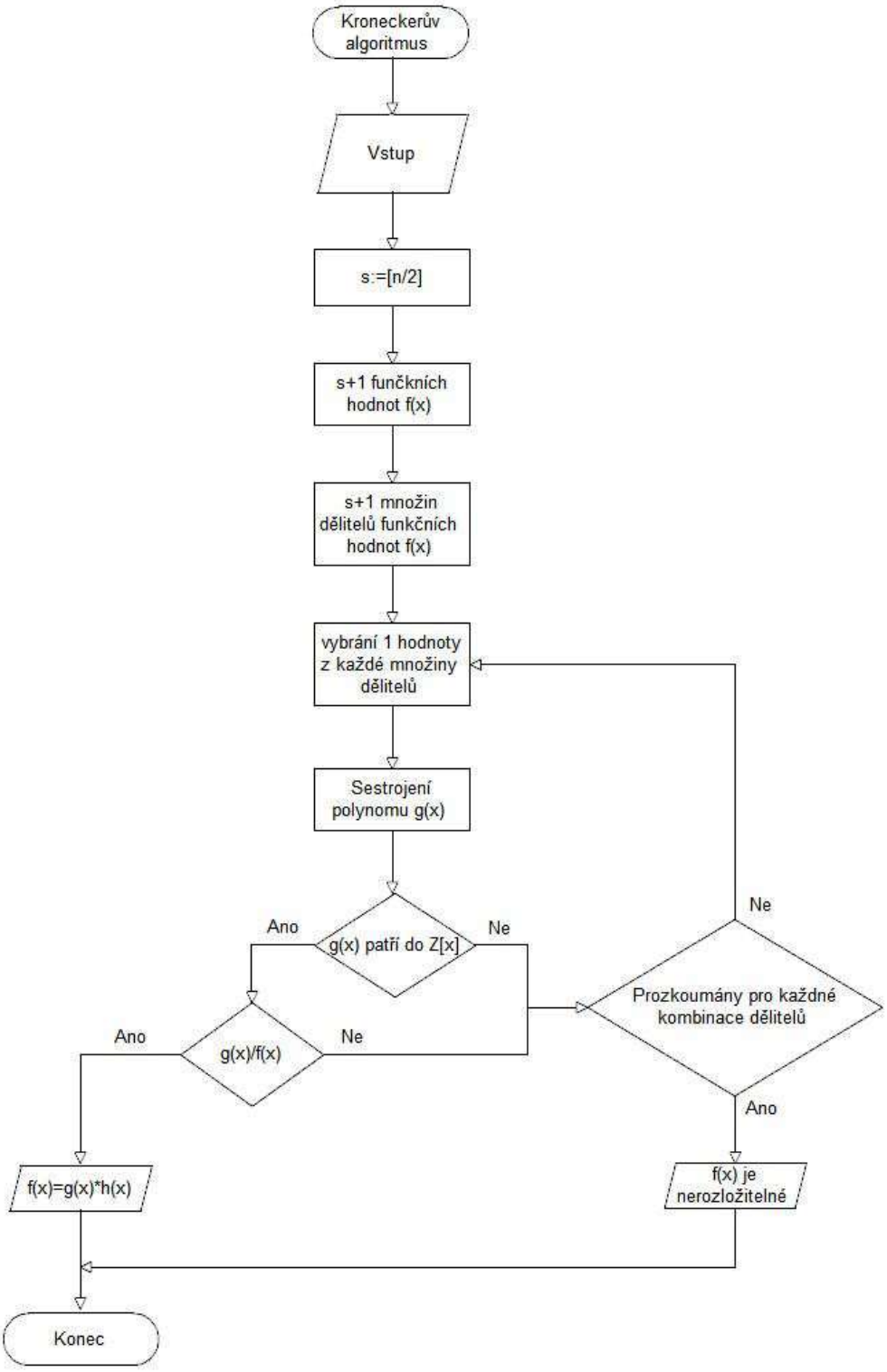
[8] Polynomy. Wikiknihy. [online]. [cit. 2016-04-01]. Dostupné z: https://cs.wikibooks.org/wiki/%C3%9Avod_do_algebry/Polynomy

[9] Polynomy. Stránky katedry matematiky ZČU FAV Plzeň. [online]. [cit. 2016-04-01]. Dostupné z: http://home.zcu.cz/~rvyrut/WWW-KMA/GS1/dalkari/polynomyN.pdf

[10] Polynom. Wikipedia: otevřená encyklopedie [online]. [cit. 2016-04-01]. Dostupné z: https://cs.wikipedia.org/wiki/Polynom#Ko.C5.99en_polynomu

[11] JANDL, Jíří. *Ireducibilita polynomů v Z[x].* Plzeň, 2013. Bakalářská práce. ZČU v Plzni. Vedoucí práce doc. RNDr. Jaroslav Hora, CSc.

Přílohy



obr.2


TEXAS INSTRUMENTS
TI-92 Plus
LOCK
F1
F2
F3
F4
F5
F6
F7
F8
2nd
QUIT
ESC
MODE
CLEAR
APPS
ENTER
LN
SIN
COS
TAN
HOME
WINDOW
GRAPH
TABLE
UNITS
CAPS
ENTRY
INS DEL
OFF
ON
RCL
STO
MATH
MEM
VAR-LINK
EE
CATALOG
CUSTOM
CHAR
ANS

obr.3