ZÁPADOČESKÁ UNIVERZITA V PLZNI

FAKULTA PEDAGOGICKÁ

KATEDRA MATEMATIKY, FYZIKY A TECHNICKÉ VÝCHOVY

IREDUCIBILITA POLYNOMŮ V Z(x)

BAKALÁŘSKÁ PRÁCE

JIŘÍ JANDL

Přírodovědná studia, Matematická studia

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

Plzeň 2013

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

Plzeň, 13. února 2013

.....

vlastnoruční podpis

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

Obsah

ÚVOD

V této bakalářské práci se budeme zabývat ireducibilitou, neboli nerozložitelností polynomů s celočíselnými koeficienty. Faktorizace polynomů, nebo chceme-li také řešení polynomiálních rovnic, je jedním z nejstarších problémů, kterými se matematika, respektive algebra, zabývá. Původně šlo vlastně o hledání kořenů či kořenových činitelů. V této práci si vysvětlíme pojmy ireducibilní a reducibilní mnohočlen a vysvětlíme některé algoritmy, které se dají použít k zjištění daných vlastností.

V první kapitole si připomeneme základní věty a definice, které se týkají polynomů. Potom si připomeneme základní operace s polynomy. Větší pozornost budeme věnovat podílu polynomů.

V druhé kapitole si vysvětlíme pojmy ireducibility a reducibility polynomů, kde hlavní tématikou je Eisensteinovo kritérium ireducibility polynomu v $\mathbb{Z}[x]$. Toto kritérium si uvedeme i s důkazem a předvedeme na několika příkladech.

V třetí kapitole se budeme zabývat rozkladem polynomu čtvrtého stupně. Tato metoda byla již známa koncem 19. století. V dnešní době není obvyklé se s ní setkat v učebnicích moderní algebry. Rozklad polynomu je „ ručně ‘‘ poměrně náročný. Metodu pro tento rozklad si ukážeme a předvedeme ve stručnosti i na příkladech.

Ve čtvrté kapitole si ukážeme, jak lze rozložit polynom pomocí Kroneckerova algoritmu. V roce 1882 přišel Leopold Kronecker s algoritmem, který dokázal určit rozklad libovolného polynomu v $\mathbb{Z}[x]$, ale tento postup je poněkud nepraktický, i když dovedl konstatovat, že polynom je ireducibilní.

V poslední kapitole si vysvětlíme čtyři různé algoritmy pro rozklad polynomu v součinu faktorů nedělitelných čtvercem. Tyto algoritmy si podrobně vysvětlíme a předvedeme na příkladech.

První kapitola

1.1. Polynomy a operace s nimi

Polynomy nazýváme také jako mnohočleny, se kterými jsme se již seznámili na základní škole a posléze i na střední škole. Nejprve si nadefinujeme pojem polynomu a pak si připomeneme základní operace s mnohočleny.

Definice 1.1. (Polynom)

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

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

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

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

Definice 1.2. (Primitivní polynom)

Nenulový polynom (zapsaný v obecném tvaru) $f(x)=a_n x^n+a_{n-1}x^{n-1}+...+a_2x^2+a_1x^1+a_0$, kde koeficienty polynomu a_n, $a_{n-1},\ldots,$ a_1, $a_0\in\mathbb{Z}$ se nazývá primitivní polynom, právě když jeho koeficienty jsou nesoudělné, tj. když největší společný dělitel $D(a_0,a_1,...,a_{n-1},a_n)=1$.

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

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

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

Příklad 1.1.

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

Řešení:

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

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

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

Příklad 1.2.

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

Řešení:

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

Další základní operací je dělení polynomu polynomem, které nelze definovat jako předešlé operace, proto se budeme podrobněji touto tématikou více zabývat v následující kapitole 1.2.

1.2. Dělitelnost polynomů

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

Věta 1.1.

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

Příklad 1.3.

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

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

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

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

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

$$\left(2x^4 - 3x^3 + 4x^2 + 5x + 5\right) : \left(x^2 - 3x + 2\right) = 2x^2 + 3x + 9$$
$$-\left(2x^4 - 6x^3 + 4x^2\right)$$

$$3x^3 + 5x + 5$$
$$-\left(3x^3 - 9x^2 + 6x\right)$$

$$9x^2 - x + 5$$

$$-\left(9x^2 - 27x + 5\right)$$

$$26x - 13$$

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

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

Příklad 1.4.

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

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

Řešení: Toto řešení příkladu je stejné jako v příkladě **1.3**.

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

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

$$-\left(x^5 - 2x^4 + x^3 - 5x^2\right)$$

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

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

$$0$$

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

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

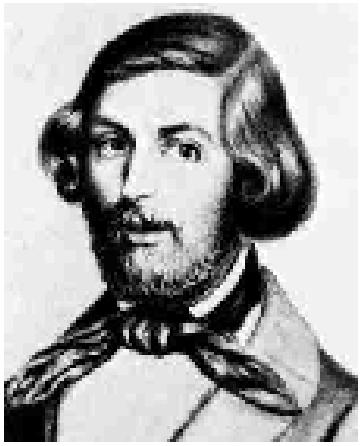
Platí tedy $x^5-2x^4-4x^3+5x^2-5x+25=(x^3-2x^2+x-5)\cdot(x^2-5)$.

Druhá kapitola

2.1. Pojem ireducibilita polynomu

Pro připomenutí si zopakujeme ve stručnosti teoretické základy vyšetřované problematiky. Je známo, že obor integrity polynomů $\mathbb{Z}[x]$ s celočíselnými koeficienty je oborem integrity s jednoznačným rozkladem. To znamená, že každý nenulový prvek tohoto oboru integrity, který není jednotkou ve smyslu dělitelnosti, může být zapsán jako součin konečně mnoha ireducibilních prvků. Tito činitelé jsou přitom určeny jednoznačně až na pořadí a na asociované prvky. Z druhé strany připomeňme, že v $\mathbb{Z}[x]$ obecně nelze k určení největšího společného dělitele užít Euklidův algoritmus. To znamená, že v $\mathbb{Z}[x]$ není euklidovským oborem integrity a není ani oborem integrity hlavních ideálů. Zde je otázkou, jak rozeznat prvek v $\mathbb{Z}[x]$, který je ireducibilní nebo nikoli.

Ferdinand Gotthold Max Eisenstein



Narodil se 16. dubna 1823 v Berlíně do rodiny, která ještě před jeho narozením konvertovala od judaismu ke křesťanství. Měl šest sourozenců a jako jediný z nich přežil zápal mozkových blan, který je v dětství postihl. Ve svých čtrnácti letech nastoupil na Gymnázium Friedricha Wilhelma a následně přestoupil na Gymnázium Friedricha Werdera v Berlíně. Jeho učitelé rozpoznali jeho matematický talent a všemožně jej podporovali. V roce 1843 byl přijat na Univerzitu Friedricha Wilhelma (nyní Humboltova Univerzita v Berlíně) a během dalšího roku zveřejnil dvacetpět svých článků v matematickém časopise Augusta Leopolda Crella. Crell jej představil Alexandru von Humboltovi, který se stal jeho celoživotním

kantorem a sponzorem a také ho seznámil s Karlem Friedrichem Gaussem. V roce 1847 se stal profesorem matematiky a krátce před svou smrtí byl zvolen do Royal Prussian Academy of Sciences and Humanities. Zemřel 11. října 1852 na tuberkulózu.

2.2. Eisensteinovo kritérium ireducibility

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

Definice 2.1.

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

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

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

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

Věta 2.1. (Eisensteinovo kritérium ireducibility)

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

i) p nedělí a_n,

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

iii) p^2 nedělí a_0.

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

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

Důkaz: Provedeme sporem.

Z dokázaného kritéria můžeme nanejvýš vytknout celočíselnou konstantu tzv. polynom stupně nula. Druhým důvodem pro reducibilitu polynomu $f(x) \in \mathbb{Z}[x]$ může být, že jej lze zapsat jako součin dvou polynomů kladných stupňů s celočíselnými koeficienty. Pokud budou splněny podmínky pro jisté prvočíslo p Eisensteinova kritéria ireducibility (i), (ii), (iii) a je –li testovaný polynom primitivní, pak polynom je ireducibilní v $\mathbb{Z}[x]$. Ukážeme si na několika příkladech.

Příklady 2.1.

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

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

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

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

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

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

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

Pokud budeme studovat rozložitelnost polynomů v $\mathbb{Z}[x]$, mohlo by se zdát, že je příliš omezující. Existuje však úzká souvislost mezi rozložitelností v $\mathbb{Z}[x]$ a v oboru integrity polynomů s racionálními koeficienty $\mathbb{Q}[x]$. Jak již víme, postačí nám zkoumat faktorizaci primitivních polynomů.

Věta 2.2.

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

$h_1(x) \in \mathbb{Z}[x]$ takové, že $f(x) = g_1(x) \cdot h_1(x)$. Přitom platí $g(x) = a \cdot g_1(x)$, $h(x) = b \cdot h_1(x)$, $a,\ b \in \mathbb{Q}$, $a \cdot b = \pm 1$.

Třetí kapitola

3.1. Faktorizace polynomů čtvrtého stupně

Nyní se budeme zabývat rozkladem polynomů čtvrtého stupně. Tato faktorizace polynomů již byla zmíněna v roce 1886 v algebraické literatuře. V moderní době technika rozkladu polynomů čtvrtého stupně nad racionálními čísly není obvykle diskutována v učebnicích moderní algebry. Zdá se tedy, že faktorizační teorie pro polynomy čtvrtého stupně je již zapomenuta, proto si ji připomeneme.

Rozložit polynom třetího stupně určitě dovedeme, např. $f(x) = x^3 - 4x^2 + 4x - 3$ na $(x-3)(x^2 - x + 1)$, tedy $f(x)$ má netriviální rozklad a je tudíž reducibilní. Avšak obtížnější je faktorizace polynomu čtvrtého stupně, např. $x^4 - 8x^3 + 22x^2 - 19x - 8$.

Základní nástroje pro rozklad polynomů jsou:

Věta 3.1. (O činiteli neboli faktoru)

Nechť $f \in \mathbb{Q}[x]$ a $c \in \mathbb{Q}$. Pak je kořenem polynomu $f(x)$, tj. platí $f(c) = 0$, jestliže $x - c$ je činitelem $f(x)$.

Věta 3.2. (O racionálních kořenech)

Nechť $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$, kde koeficienty $a_n, a_{n-1}, \ldots, a_0$ jsou celá čísla. Jestliže $\mathrm{p} \mid q$ je racionální číslo v základním tvaru takové, že $f(\mathrm{p} \mid q) = 0$, pak p dělí a_0 a q dělí a_n.

Tyto věty dostačují pro rozklad jakéhokoli polynomu druhého a třetího stupně. Tyto polynomy jsou reducibilní právě tehdy, když mají nějaký kořen v $\mathbb{Q}$. Nalezení takového kořene je snadné díky větě o racionálních kořenech a pak dlouhé dělení poskytuje odpovídající faktorizaci.

Polynomy čtvrtého stupně lze někdy rozložit na součin dvou polynomů druhého stupně, které nemají kořeny z $\mathbb{Q}$, tj. nemají pochopitelně lineární faktory (činitele). Pak k určení, zda je, nebo není polynom čtvrtého stupně bez racionálních kořenů reducibilní, potřebujeme vědět, jestli je rozložitelný na součin dvou kvadratických polynomů. Věta 3.3 ukazuje, že tato otázka může být zodpovězena použitím asociovaného (sdruženého) polynomu třetího stupně, který se nazývá pomocný polynom (rezolventa).

Pro zjednodušení budeme brát v úvahu jen polynomy ve tvaru: $f(x) = ax^4 + bx^3 + cx^2 + dx + e \in \mathbb{Q}[x]$, kde $a \neq 0$, je libovolný polynom čtvrtého stupně, pak zjednodušený tvar je polynom je

$$\frac{f(x - b/4a)}{a}.$$

Např. zjednodušený tvar polynomu

$f(x) = x^4 + 8x^3 + 22x^2 - 19x - 8$ je $f(x+2) = x^4 - 2x^2 + 5x - 6.$

Zjednodušený tvar má koeficient u členu x^4 roven 1 a nemá člen třetího stupně. Snadno vidíme, jak faktorizace zjednodušeného tvaru dává faktorizaci původního polynomu. Pak toto lze zobecnit v následující větě za předpokladu, že $f(x)$ je vždy ve zjednodušeném tvaru

$$f(x) = x^4 + cx^2 + dx + e.$$

Za těchto okolností pomocný polynomu je polynom třetího stupně

$$R(z) = z^3 + 2cz^2 + (c^2 - 4e)z - d^2.$$

Pak je jednoduché počítat kořeny polynomu $f(x)$, když je rozložen; není překvapení, že pomocný polynom se objevuje v mnoha vydaných metodách pro nalezení kořenů polynomů čtvrtého stupně. Dále píšeme $\mathbb{Q}^2 = \{s^2 \mid s \in \mathbb{Q}\}$ pro čtverce z $\mathbb{Q}^2$.

Věta 3.3.

Polynom čtvrtého stupně $f(x) = x^4 + cx^2 + dx + e \in \mathbb{Q}[x]$ se rozloží na kvadratické polynomy z $\mathbb{Q}[x]$ právě tehdy, když je splněna alespoň jedna podmínka:

(A) pomocný polynom R má nenulový kořen z $\mathbb{Q}^2$.

(B) $d=0$ a $c^2-4e\in\mathbb{Q}^2$.

Důkaz:

Předpokládejme, že $f(x)$ se rozloží jako $f(x)=\left(x^2+hx+k\right)\cdot\left(x^2+h'x+k'\right)$ (1), kde $h,h',k,k'\in\mathbb{Q}$ vynásobením (1) a spojením koeficientů dostaneme $0=h+h',\ e=kk'$ (2), $d=hk'+h'k,\quad c=hh'+k+k'$ (3). Pak $h'=-h$ a rovnice (3) je lineární, kde k a k' mohou být rozděleny do bloků $2hk=h^3+ch-d,\quad 2hk'=h^3+ck+d$ (4). Z $e=kk'$ a (4) dostaneme $4h^2e=(2hk)(2hk')=\left(h^3+ch-d\right)\left(h^3+ch+d\right)$ (5). Vynásobením dostaneme

$h^6+2ch^4+\left(c^2-4e\right)h^2-d^2=0$ (6) a tak h^2 je kořen pomocného polynomu R. Jestliže $h\neq 0$, pak platí z věty 4.3 (A). Jestliže $h=0$, pak z (6) vyplývá, že $d=0$ a z (2) a (3) dostaneme $c^2-4e=\left(k+k'\right)^2-4kk'=\left(k-k'\right)^2\in\mathbb{Q}^2$. V tomto případě platí (B) věty 4.3.

Nyní budeme předpokládat, že pomocný polynom R je nenulový kořen z $\mathbb{Q}^2$. Pak existuje nějaké nenulové $h\in\mathbb{Q}$ takové, že platí (6). Rovnice $h'=-h,\quad k=\frac{1}{2h}\left(h^3+ch-d\right)$, $k'=\frac{1}{2h}\left(h^3+ch+d\right)$ (7). Pak $h',k,k'\in\mathbb{Q}$ a z (6) vyplývá (5), platí rovnice (2) a (3). Pak $f(x)$ se rozloží na kvadratické polynomy z $\mathbb{Q}[x]$ jako v (1). Předpokládejme, že $d=0$ a $c^2-4e=\mathrm{s}^2$ pro libovolné $\mathrm{s}\in\mathbb{Q}$. Rovnice $h=h'=0,\ k=\frac{(c+\mathrm{s})}{2}$ a $k'=\frac{(c-\mathrm{s})}{2}$ (8). Pak $h',h,k,k'\in\mathbb{Q}$ a $k+k'=c,\ kk'=\frac{\left(c^2-s^2\right)}{4}=e,\ f(x)=\left(x^2+k\right)\left(x^2+k'\right)$ a potom se opět $f(x)$ rozloží na kvadratické polynomy z $\mathbb{Q}[x]$.

Z důkazu této věty můžeme získat algoritmus pro rozklad polynomu čtvrtého stupně $f(x)$ ve zjednodušeném tvaru. Nejdříve pomocí věty o racionálních kořenech najdeme racionální kořeny $f(x)$. Jestliže $c\in\mathbb{Q}$ je takový kořen, že splňuje podmínku z věty o faktoru, pak víme, že $f(x)=(x-\mathrm{c})\cdot\mathrm{g}(x)$ pro libovolné polynomy třetího stupně $g(x)$, které mohou být

určeny dělením. Jestliže $f(x)$ nemá racionální kořeny, pak hledáme racionální kořeny pomocného polynomu R. Jestliže $h^2 \in \mathbb{Q}^2$ je nenulový kořen rezolventy R, pak platí podmínka věty 4.3 (A) a rovnice (7) a (1) dají faktorizaci polynomu $f(x)$. Jestliže platí (B) věty 3.3 pak rovnice (8) a (1) určují faktorizaci polynomu $f(x)$. Jestliže tyto kroky nevedou k faktorizaci, pak polynom $f(x)$ je ireducibilní.

Příklad 3.1.

Je dán polynom $f(x) = x^4 + x^2 + x + 1$. Pak polynom $f(x)$ a ani pomocný polynom $R(z) = z^3 + 2z^2 - 3z - 1$ nemá racionální kořen, tudíž polynom $f(x)$ je ireducibilní.

Příklad 3.2.

Polynom $f(x) = x^4 + 2x^2 + 5x + 11$. Pak $f(x)$ nemá racionální kořeny a pomocný polynom $R(z) = z^3 + 4z^2 - 40z - 25$ má jeden racionální kořen, tj. hodnotu 5, který není v $\mathbb{Q}^2$ a tudíž polynom $f(x)$ je ireducibilní.

Příklad 3.3.

Polynom $f(x) = x^4 - 12x^2 - 3x + 2$. Tento polynom $f(x)$ nemá racionální kořeny, ale pomocný polynom $R(z) = z^3 - 24z^2 + 136z - 9$ má jeden racionální kořen, jmenovitě $9 \in \mathbb{Q}^2$. Pak polynom $f(x)$ je reducibilní. Dosazením $h = \sqrt{9} = 3$ do rovnic (7) a (1) dostaneme polynom $f(x) = (x^2 + 3x - 1)(x^2 - 3x - 2)$.

Příklad 3.4.

Polynom $f(x) = x^4 - 8x^3 + 22x^2 - 19x - 8$, motivační příklad ze začátku této kapitoly. Tento polynom $f(x)$ nemá racionální kořeny. Přejdeme na zjednodušený tvar tohoto polynomu, tj. $f(x+2) = x^4 - 2x^2 + 5x - 6$. Jeho pomocný polynom $R(z) = z^3 - 4z^2 + 28z - 25$ má jeden racionální kořen, tj. $1 \in \mathbb{Q}^2$. Dosazením $h = \sqrt{1} = 1$ do rovnic (7) a (1) dostaneme polynom. $f(x+2) = (x^2 + x - 3)(x^2 - x + 2)$. Pak dostaneme rozklad původního polynomu $f(x)$ na

dva polynomy druhého stupně $f(x)=\left(x^2-3x-1\right)\left(x^2-5x+8\right)$. Polynom $f(x)$ je tudíž reducibilní.

Tuto kapitolu zakončíme vyšetřením speciálního případu, kdy $f(x)=x^4+cx^2+e.$ Jestliže $r\in\mathbb{Q}$ je kořen polynomu $f(x)=x^4+cx^2+e$, pak také $-r$ je kořenem, a $x^2-r^2\in\mathbb{Q}[x]$ dělí polynom $f(x)$. Potom $f(x)$je reducibilní právě tehdy, když lze rozložit na dva kvadratické polynomy. Pokud $d=0$, pomocný polynom (rezolventa) polynomu $f(x)$ je $R(z)=$ $=z\left(z^2+2cz+\left(c^2-4e\right)\right)$ s kořeny 0, $-c\pm 2\sqrt{e}.$ Věta 3.3 nyní umožní zkoušku, zda je polynom $f(x)$ireducibilní.

Věta 3.4.

Polynom čtvrtého stupně $f(x)=x^4+cx^2+e\in\mathbb{Q}[x]$ je reducibilní právě tehdy, když $c^2-4e\in\mathbb{Q}^2$, nebo $-c+2\sqrt{e}\in\mathbb{Q}^2$ a nebo $-c-2\sqrt{e}\in\mathbb{Q}^2$. Pro podmínky zahrnující $\sqrt{e}$, aby platily, je nutné, aby $e\in\mathbb{Q}^2$.

Příklad 3.5.

Rozložte polynom $f(x)=x^4-3x^2+1$.

Nejprve určíme $c=-3$ a $e=1$. Máme $c^2-4e=5\notin\mathbb{Q}^2$, $-c+2\sqrt{e}=5\notin\mathbb{Q}^2$, $-c-2\sqrt{e}=1$,

$1\in\mathbb{Q}^2$. Pro výpočet faktorizace dosadíme $h=1$ do rovnic (7) a (1) a dostáváme polynom $f(x)=\left(x^2+x-1\right)\left(x^2-x-1\right)$. Tento polynom $f(x)$ je reducibilní.

Příklad 3.6.

Rozložte polynom $f(x)=x^4-16x^2+4$.

Určíme $c=-16$ a $e=4$. Máme tedy $c^2-4e=240\notin\mathbb{Q}^2$, $-c+2\sqrt{e}=20\notin\mathbb{Q}^2$, $-c-2\sqrt{e}=12$,

$12\notin\mathbb{Q}^2$. V tomto případě nenáleží hledané kořeny do $\mathbb{Q}^2$, tudíž polynom $f(x)$ je ireducibilní.

Čtvrtá kapitola

Leopold Kronecker

Klasickým algoritmem pro faktorizaci polynomů v $\mathbb{Z}[x]$ je tradičně nazýván Kroneckerův algoritmus, po německém matematikovi Leopoldu Kroneckerovi (1823 –1891), který se narodil v zámožné a vzdělané židovské rodině, jeho mladší bratr Hugo (1839-1914) byl významný fyziolog. Získal vynikající vzdělání od domácích učitelů a na gymnáziu byl jeho učitelem Ernst Eduard Kummer, který v něm probudil zájem o matematiku. Roku 1841 začal studovat filosofii na univerzitě v Berlíně, zajímal se hlavně o Descarta, Leibnize, Kanta, Hegela a Spinozu. Studoval také astronomii, chemii, meteorologii a zejména matematiku, k jeho učitelům patřili Dirichlet a Steiner. Po kratších pobytech na univerzitách v Bonnu a Vratislavi se roku 1844 vrátil do Berlína. Tam v roce 1845 promoval latinskou prací o „Komplexních jednotkách“. Pak se deset let s velkým úspěchem věnoval obchodu a zajistil si tak finanční nezávislost, také díky bohatému strýci a sňatku s jeho dcerou. Znovu začal s matematikou v roce 1853, kdy rozšířil Galoisovu teorii algebraických rovnic. Kronecker publikoval množství prací na nejrůznější témata jako teorie čísel, eliptické funkce apod. Díky těmto pracím byl roku 1860 přijat za člena berlínské Akademie. To mu dalo právo přednášet na univerzitě, kde vyučoval teorii čísel, teorii rovnic, teorii determinantů a integrálů. Nepřitahoval příliš mnoho studentů, jen málo z nich bylo schopno sledovat jeho myšlenky a dokonale jim porozumět. Mezi nimi byl například Georg Cantor a Edmund Husserl. Kronecker odmítl nabídku profesury na univerzitě v Göttingen, protože jej přitahoval Berlín, kde získal místo profesora v roce 1883 po svém někdejším učiteli Kummerovi, a kde také roku 1891 zemřel.

4.1. Kroneckerův algoritmus

Tento algoritmus je posloupnost několika kroků:

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

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

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

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

d) Pomocí $s+1$ vybraných hodnot $g(0) \in D_{f(0)}$, $g(1) \in D_{f(1)}$, …, $g(s) \in D_{f(s)}$ určíme polynom $g(x)$, který v bodě $x = 0$ nabývá vybrané hodnoty $g(0)$, v bodě $x = 1$ hodnoty $g(1)$,…, v bodě $x = s$ hodnoty $g(s)$. Tento mnohočlen $g(x)$ spočteme postupem užívaným pro nalezení tzv. Newtonova interpolačního polynomu. Při hledání Newtonova interpolačního polynomu jde v podstatě o nalezení předpisu pro mnohočlen $g(x)$ kladného stupně s, přičemž známe jeho $s+1$ funkčních hodnot $f(x_i)$, kterých nabývá v $s+1$ bodech $x_i = 0$, 1, …, s. Polynom $g(x)$ zapíšeme ve tvaru $g(x) = \lambda_0 + \lambda_1(x - x_0) + \lambda_2(x - x_0) \cdot (x - x_1) + ... + \lambda_s(x - x_0) \cdot ... \cdot (x - x_{s-1})$. Výpočet polynomu $g(x)$, respektive dopočítání koeficientů λ_0, λ_1, …, λ_s se pak dá zjednodušit zapsáním do tzv. „schématu rozdílů“:

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

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

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

$$
\begin{array}{llll}
g(x_0) & & & \\
 & \Delta g(x_0) & & \\
g(x_1) & & \Delta^2 g(x_0) & \\
 & \Delta g(x_1) & & \Delta^3 g(x_0) \\
g(x_2) & & \Delta^2 g(x_1) & \\
 & \Delta g(x_2) & & \\
g(x_3) & & &
\end{array}
$$

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

Příklad 4.1.

Nalezněte polynom nejvýše třetího stupně, pro který platí $p(0)=3$, $p(1)=1$, $p(2)=9$, $p(3)=33$.

Řešení:

Nejprve si zapíšeme známé funkční hodnoty do „schématu rozdílů“, podle výše zmíněného postupu. Dále spočteme potřebné hodnoty a z nich potom dopočteme koeficienty λ_k.

$$
\begin{array}{llll}
3 & & & \\
 & -2 & & \\
1 & & 10 & \\
 & 8 & & 6 \\
9 & & 16 & \\
 & 24 & & \\
33 & & &
\end{array}
$$

$$\lambda_0 = \frac{3}{0!} = 3,$$
$$\lambda_1 = \frac{-2}{1!} = 3,$$
$$\lambda_2 = \frac{10}{2!} = 5,$$
$$\lambda_3 = \frac{6}{3!} = 1.$$

Nyní dosadíme do rovnice tyto koeficienty:

$p(x) = \lambda_0 + \lambda_1 \cdot (x - x_0) + \lambda_2 \cdot (x - x_0) \cdot (x - x_1) + \lambda_3 \cdot (x - x_0) \cdot (x - x_1) \cdot (x - x_2)$, potom dostaneme rovnici $p(x) = 3 - 2 \cdot (x - 0) + 5 \cdot (x - 0)(x - 1) + 1 \cdot (x - 0)(x - 1)(x - 2)$, po roznásobení závorek $p(x) = x^3 + 2x^2 - 5x + 3$. Pokud zpět dosadíme do zjištěného polynomu, můžeme si ověřit, že jeho funkční hodnoty odpovídají hodnotám zadaným.

e) Takto získaný polynom nemusí být nutně z oboru mnohočlenů s celočíselnými koeficienty.

Pokud tedy $g(x) \notin \mathbb{Z}[x]$, musíme se vrátit na začátek.

f) Pokud vybereme jinou množinu hodnot $g(0), g(1), ..., g(s)$. Má-li však mnohočlen $g(x)$ všechny koeficienty celočíselné, otestujeme jej, zda v $\mathbb{Z}[x]$ dělí polynom $f(x)$. Pokud platí, že $g(x) \mid f(x)$, je úloha vyřešena a nalezli jsme rozklad $f(x) = g(x) \cdot h(x)$, $g(x), h(x) \in \mathbb{Z}[x]$, $st(g) > 0, st(h) > 0$. Nastane-li případ, že mnohočlen $g(x)$ nedělí $f(x)$, pak je nutno se vrátit na začátek oddílu d).

Opakujeme-li postup s jinou množinou funkčních hodnot $g(0), g(1), ..., g(s)$ a pokud vyzkoušíme všech $(s+1) - tic$ a přesto se nám nepodaří nalézt hledaný polynom $g(x)$, můžeme konstatovat, že polynom $f(x)$ je nerozložitelný neboli ireducibilní v oboru $\mathbb{Z}[x]$.

Příklad 4.2.

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

Řešení: Stupeň polynomu $f(x)$ je $st(f)=5$, hledaný mnohočlen $g(x)$ tedy bude mít stupeň nejvýše $st(g)=s=\left[\frac{5}{2}\right]=2$. Nyní spočítáme $(s+1)$ (v tomto případě je $s+1=3$) funkčních hodnot $f(x)$: $f(0)=1$, $f(1)=9$, $f(2)=105$ a utvoříme množiny jejich dělitelů.

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

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

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

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

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

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

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

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

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

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

a po dosazení do vzorce $g(x) = \lambda_0 + \lambda_1(x - x_0) + \lambda_2(x - x_0)(x - x_1)$ dostaneme $g(x) = 1 + 0 \cdot (x - 0) - 1 \cdot (x - 0)(x - 1)$, což po roznásobení závorek dává $g(x) = -x^2 + x + 1$. Tento polynom $g(x)$ má sice stupeň $st(g) = 2$ a je i z oboru $\mathbb{Z}[x]$, avšak vydělíme-li jím mnohočlen $f(x)$, nedostaneme nulový zbytek. Polynom $g(x)$ tedy není dělitelem polynomu $f(x)$.

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

1		
	2	
3		2
	4	
7		

Koeficienty λ_k jsou

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

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

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

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

Tento mnohočlen již v $\mathbb{Z}[x]$ dělí polynom $f(x)$ beze zbytku. To znamená, že jsme nalezli rozklad polynomu $f(x)$ na dva mnohočleny nižších stupňů a můžeme psát

$f(x) = x^5 + 3x^4 + 2x^3 + 2x^2 + 1 = (x^2 + x + 1) \cdot (x^3 + 2x^2 - x + 1) = g(x) \cdot h(x)$, kde mnohočlen $g(x)$, $h(x) \in \mathbb{Z}$ a $st(g) \geq 1$, $st(h) \geq 1$, čímž jsme tento příklad vyřešili a zjistili, že daný polynom je reducibilní.

Příklad 4.3.

Rozhodněte v $\mathbb{Z}[x]$ o reducibilitě či ireducibilitě polynomu

$$f(x) = 2x^7 + 3x^6 - 11x^5 - 8x^4 + 21x^3 + 6x^2 - 15x + 3.$$

Řešení: Stupeň polynomu $f(x)$ je $st(f) = 7$, takže $s = \left[\frac{7}{2}\right] = 3$. Hledáme polynom $g(x)$ nejvýše kubický. Potřebujeme $(s+1) = 4$ pro několik vybraných čtveřic $[g(0), g(1), g(2), g(3)]$ funkčních hodnot $f(x)$: $f(0) = 3$, $f(1) = 1$, $f(2) = 133$, $f(3) = 3819$, ke kterým sestrojíme množiny dělitelů.

$D_{f(0)} = \{1, -1, 3, -3\}$,

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

$D_{f(2)} = \{1, -1, 7, -7, 19, -19, 133, -133\}$,

$D_{f(3)} = \{1, -1, 3, -3, 19, -19, 57, -57, 67, -67, 201, -201, 1273, -1273, 3819, -3819\}$

V nejhorším případě bychom pro nalezení rozkladu polynomu $f(x)$ museli projít všech 1024 uspořádaných čtveřic, neboť $4 \cdot 2 \cdot 8 \cdot 16 = 1024$. Zvolíme tedy například hodnoty $g(0) = 1$, $g(1) = 1$ a $g(2) = g(3) = 1$, máme ovšem $g(x) = 1$, a tím nemusíme dosazovat do „schématu rozdílu“. Povšimněme si, že interpolační polynom nemusí mít právě stupeň $s = 3$, ale může mít i stupeň nižší. V tomto případě jde o konstantu a nalezli jsme triviální dělitel $g(x) = 1$ polynomu $f(x)$. A tím je nutné pokračovat v hledání vhodných množin dělitelů.

Zvolíme dalších několik vybraných čtveřic $[g(0), g(1), g(2), g(3)]$.

Hodnoty $g(0)=1,\ g(1)=1,\ g(2)=7,\ g(3)=-19$ dosadíme do „schématu rozdílu“.

1			
	0		
1		6	
	6		–38
7		–32	
	–26		
–19			

Koeficienty λ_k potom budou

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

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

$$\lambda_2 = \frac{6}{2!} = 3,$$

$$\lambda_3 = -\frac{38}{3!} = -\frac{19}{3}.$$

Dosadíme je do vzorce a dostaneme

$$g(x) = 1 + 0\cdot(x-0) + 3\cdot(x-0)(x-1) - \frac{19}{3}\cdot(x-0)(x-1)(x-2),$$

po roznásobení máme $g(x) = -\frac{19}{3}x^3 + 22x^2 - \frac{47}{3}x + 1$. Tento mnohočlen ovšem nepatří do oboru $\mathbb{Z}[x]$, protože nemá všechny koeficienty celočíselné, takže se vrátíme zpět k výběru hodnot z množin dělitelů a zvolíme jiné.

3) Pro několik vybraných čtveřic $[g(0),\ g(1),\ g(2),\ g(3)]$.

Hodnoty $g(0)=1,\ g(1)=1,\ g(2)=19,\ g(3)=57$ dosadíme opět do „schématu rozdílu“.

1

0

1 18

18 2

19 20

38

57

Opět určíme koeficienty λ_k :

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

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

$$\lambda_2 = \frac{18}{2!} = 9,$$

$$\lambda_3 = \frac{2}{3!} = \frac{1}{3}.$$

Dosadíme je do vzorce a dostaneme

$$g(x) = 1 + 0 \cdot (x-0) + 9 \cdot (x-0)(x-1) + \frac{1}{3} \cdot (x-0)(x-1)(x-2),$$

po roznásobení máme $g(x) = \frac{1}{3}x^3 + 8x^2 - \frac{25}{3}x + 1$. Tento mnohočlen opět nepatří do oboru $\mathbb{Z}[x]$, protože nemá všechny koeficienty celočíselné, takže se vrátíme zpět k výběru hodnot z množin dělitelů a zvolíme jiné.

4) Pro několik vybraných čtveřic $\left[g(0),\ g(1),\ g(2),\ g(3)\right]$.

Hodnoty $g(0) = 1,\ g(1) = 1,\ g(2) = 19,\ g(3) = 67$ a dosadíme opět do „schématu rozdílu“.

1

0

1 18

18 12

19 30

48

67

Vypočteme koeficienty λ_k :

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

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

$$\lambda_2 = \frac{18}{2!} = 9,$$

$$\lambda_3 = \frac{12}{3!} = 2.$$

Dosadíme je do vzorce a dostaneme

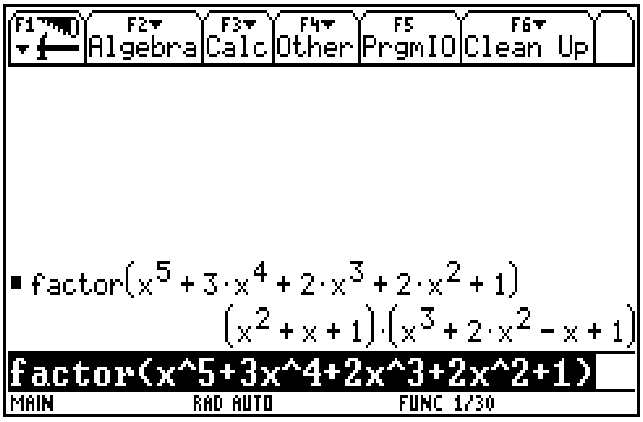
$$g(x) = 1 + 0 \cdot (x-0) + 9 \cdot (x-0)(x-1) + 2 \cdot (x-0)(x-1)(x-2),$$

po roznásobení dostáváme $g(x) = 2x^3 + 3x^2 - 5x + 1,\ g(x) \in \mathbb{Z}[x]$. Tento mnohočlen má tedy všechny koeficienty celočíselné. Pokud budeme dělit mnohočlen $f(x)$ mnohočlenem $g(x)$ zjistíme, že podíl vyjde beze zbytku a můžeme tedy psát

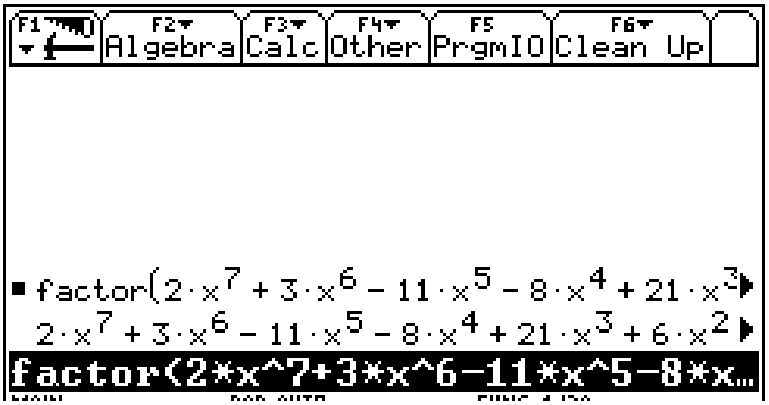
$$f(x) = (2x^3 + 3x^2 - 5x + 1)(x^4 - 3x^2 + 3) = g(x) \cdot h(x),$$

kde $g(x),\ h(x) \in \mathbb{Z}[x],\ st(g) \geq 1,\ st(h) \geq 1$. Aplikujeme-li navíc na oba polynomy $g(x)$, $h(x)$ Eisensteinovo kritérium ireducibility, zjistíme pomocí prvočísla $p = 2$, že oba polynomy jsou ireducibilní. Dostali jsme tedy úplný rozklad polynomu $f(x)$, což znamená, že tento polynom je rozložitelný, tzv. reducibilní.

Obrázky, které jsme pořídili na kalkulátoru TI -92 Plus a využili jsme právě Kroneckerova algoritmu.



Obrázek 1



Obrázek 2

Zatímco na obrázku 1 je případ, kdy se rozklad polynomu pátého stupně podařilo na kalkulátoru TI -92 Plus nalézt, vidíme na obrázku 2, že stejný typ kalkulátoru již u polynomu sedmého stupně úspěšný nebyl. Důvodem je zřejmě omezená paměť kalkulátoru, případně omezení pro čas výpočtu. Kroneckerův algoritmus lze tedy na „malých" kalkulátorech úspěšně provádět zhruba nanejvýš pro polynomy 6. stupně s „nevelkými" celočíselnými koeficienty.

Pátá kapitola

5.1. Square-free factorization

Square – free decomposition, je dalším algoritmem počítačové algebry. Jedná se o rozklad polynomu na součin faktorů nedělitelných čtvercem. V tomto algoritmu však nejde o úplnou faktorizaci, neboť ta vede k rozkladu mnohočlenu v součin ireducibilních faktorů. Poznamenejme, že ani tento algoritmus nemusí vždy dosáhnout úspěchu. Tento rozklad je zpravidla jednodušší a tím pádem i rychlejší než úplný rozklad, k jeho provedení stačí znalost určení formálních derivací a zároveň největších společných dělitelů. Jedná se o předstupeň k úplné faktorizaci, nicméně v některých situacích je Square – free rozklad i sám o sobě užitečný, například když je nutné určit, zda je daný polynom $n-tou$ mocninou polynomu jiného.

Definice 5.1.

Primitivní mnohočlen $v(x) \in I[x]$, $I[x]$ je obor integrity s jednoznačným rozkladem, není dělitelný čtvercem, pokud v $I[x]$ neexistuje takový polynom $u(x)$, $st(u) > 0$, pro který platí $u^2(x) \mid v(x)$.

Definice 5.2.

Nechť $f(x)$ je primitivní polynom v $I[x]$. Tento polynom je rozložitelný v součin faktorů nedělitelných čtvercem, pokud jej lze zapsat ve tvaru $f(x) = v_1^1(x) \cdot v_2^2(x) \cdot ... \cdot v_k^k(x)$, kde mnohočleny $v_i \in I[x]$ nejsou dělitelné čtvercem a jsou po dvou nesoudělné, $D(v_i, v_j) = 1$, pro všechna $i, j = 1, 2, ..., k, i \neq j$.

Poznámka: Skutečnost, kterou nesmíme opomenout je, že ireducibilita polynomu přímo implikuje jeho netriviální nerozložitelnost v součin faktorů nedělitelných čtvercem. Opačná implikace totiž neplatí (polynom může být nerozložitelný ve square-free decomposition, ale to ovšem neznamená důkaz ireducibility).

Příklad 5.1.

1) Polynom $f(x) = x^2 + 1$ je triviálně rozložitelný na součin faktorů nedělitelných čtvercem, neboť stačí položit $v_1(x) = x^2 + 1$ a zároveň je ireducibilní.

2) Polynom $f(x) = x^2 - 1$ je triviálně rozložitelný v součin faktorů nedělitelných čtvercem. Ten faktor bude opět jediný, je $v_1(x) = x^2 - 1$ a lze jej rozložit v součin $x^2 - 1 = (x+1) \cdot (x-1)$.

3) Polynom $f(x) = x^2 - 2x + 1$ je rozložitelný v součin faktorů nedělitelných čtvercem, je totiž $v_1(x) = 1$, $v_2(x) = x - 1$ a také lze provést jeho úplnou faktorizaci $f(x) = x^2 - 2x + 1 = .$

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

K nalezení rozkladu polynomu v součin faktorů nedělitelných čtvercem ke square-free rozkladu využijeme formální derivaci, jak už bylo zmíněno na začátku této kapitoly.

Formální derivace není konstruována pomocí pojmu limity funkce, jak je tomu v matematické analýze, nicméně vlastnosti obou typů derivací jsou shodné.

Definice 5.3.

Formální derivací polynomu $f(x)=a^n x_n + a^{n-1}x_{n-1}+\ldots+a_1 x+a_0$, $f(x)\in I[x]$, rozumíme polynom $f'(x)=n\cdot a_n x^{n-1}+(n-1)\cdot a_{n-1}x^{n-2}+\ldots+2a_2 x+a_1$, $f'(x)\in I[x]$.

Tato formální derivace má stejné vlastnosti jako derivace založená na limitě funkce.

Věta 5.1.

Mějme polynomy $f(x)$ a $g(x)\in I[x]$, libovolnou konstantu $k\in I$, I je obor integrity, a proměnnou $n\in\mathbb{N}$. Potom platí:

a) $[k\cdot f(x)]' = k\cdot f'(x)$, tj. z derivace mnohočlenu lze vytknout libovolnou konstantu *k*, která je dělitelem všech koeficientů tohoto mnohočlenu,

b) $[f(x)+g(x)]' = f'(x)+g'(x)$, tj. derivace součtu polynomů je rovna součtu derivací jednotlivých polynomů, kde v prvém sčítanci se vyskytuje derivace polynomu $f(x)$ a polynom $g(x)$ a ve druhém sčítanci je polynom $f(x)$ násobený derivací mnohočlenu $g(x)$, obecně pak pro n polynomů platí:

$$[f_1(x)\cdot f_2(x)\cdot\ldots\cdot f_n(x)]' =$$
$$= f_1'(x)\cdot f_2(x)\cdot\ldots\cdot f_n(x)+f_1(x)\cdot f_2'(x)\cdot\ldots\cdot f_n(x)+f_1(x)\cdot f_2(x)\cdot\ldots\cdot f_n'(x)$$

c) $[f(x)\cdot g(x)]' = f'(x)\cdot g(x)+f(x)\cdot g'(x)$, tj. derivace součinu dvou polynomů *f* (*x*) a $g(x)$ je rovna součtu dvou součinů, kde v prvém sčítanci se vyskytuje derivace polynomu $f(x)$ a polynom $g(x)$ a ve druhém sčítanci je polynom $f(x)$ násobený derivací mnohočlenu $g(x)$, obecně pak pro n polynomů platí:

$$[f_1(x)\cdot f_2(x)\cdot\ldots\cdot f_n(x)]' =$$
$$= f_1'(x)\cdot f_2(x)\cdot\ldots\cdot f_n(x)+f_1(x)\cdot f_2'(x)\cdot\ldots\cdot f_n(x)+f_1(x)\cdot f_2(x)\cdot\ldots\cdot f_n'(x)$$

d) $[f^n(x)]' = n\cdot f^{n-1}(x)\cdot f'(x)$, tj. umocněný polynom je v podstatě složená funkce a derivuje se tedy stejným způsobem, což znamená: Nejprve derivujeme vnější funkce, v našem případě je umocnění polynomu, a výsledek se násobí derivací vnitřní funkce, kterou je samotný polynom.

Tuto větu použijeme v následující úvaze:

Pokud je polynom $f(x) \in I[x]$ dělitelný čtvercem nějakého polynomu $v(x) \in I[x]$, přičemž $st(v) \geq 1$, lze jej zapsat ve tvaru $f(x) = u(x) \cdot v^2(x)$, jeho derivace je $f'(x) = u'(x) \cdot v^2(x) + u(x) \cdot 2v(x) \cdot v'(x)$. Tento zápis derivace můžeme upravit, pokud z obou sčítanců je možné vytknout právě polynom $v(x)$: $f'(x) = v(x) \cdot [u'(x) \cdot v(x) + 2 \cdot u(x) \cdot v'(x)]$. Jelikož derivací mnohočlenu a rovněž derivací součtu, rozdílu či součinu polynomů je opět polynom, tudíž lze zjednodušit zápis do tvaru $f'(x) = v(x) \cdot w(x)$, kde $w(x) = u'(x) \cdot v(x) + 2 \cdot u(x) \cdot v'(x)$. Vzhledem k tomu, že v obou polynomech, v $f(x)$ i jeho derivaci $f'(x)$, se vyskytuje faktor $v(x)$, nejsou $f(x)$ a $f'(x)$ nesoudělné, tj. $D(f(x), f'(x)) \neq 1$.

Zároveň při postupu „z druhé strany“ můžeme tvrdit, že nejsou-li polynomy $f(x)$ a $f'(x)$ nesoudělné, tedy $D(f(x), f'(x)) \neq 1$, je polynom $f(x)$ dělitelný čtvercem nějakého polynomu.

Důkaz: Provedeme sporem.

Předpokládáme, že polynomy $f(x)$ a $f'(x)$, $f(x) \in I[x]$, $f'(x) \in I[x]$, nejsou nesoudělné, tj. $D(f(x), f'(x)) \neq 1$, a rovněž $f(x)$ není dělitelný čtvercem žádného polynomu z oboru integrity $I[x]$.

Rozklad tohoto polynomu $f(x)$ lze tedy zapsat vztahem $f(x) = g_1(x) \cdot g_2(x) \cdot \ldots \cdot g_n(x)$, kde pro všechny polynomy $g_i(x)$, $i = 1, 2, ..., n$, platí, že g_i je ireducibilní polynom, $st(g_i) \geq 1$ a každé dva polynomy g_i a g_j jsou nesoudělné pro všechna $i, j = 1, 2, \ldots, n$, $i \neq j$. Derivujeme-li mnohočlen $f(x)$, dostaneme rovnici:

$$f'(x) = g_1'(x) \cdot g_2(x) \cdot \ldots \cdot g_n(x) + g_1(x) \cdot g_2'(x) \cdot \ldots \cdot g_n(x) + \ldots + g_1(x) \cdot g_2(x) \cdot \ldots \cdot g_n'(x).$$

Jelikož $f(x)$ a $f'(x)$ nejsou nesoudělné, musí platit, že alespoň jeden z faktorů g_i, $i = 1, 2, ..., n$, dělí $f(x)$ i $f'(x)$. Bez újmy na obecnosti můžeme předpokládat, že tímto faktorem je mnohočlen g_1 (pokud by jím byl některý z ostatních faktorů, provedli bychom jejich přečíslování).

V tom případě tedy g_1 musí dělit součet $g_1'(x)\cdot g_2(x)\cdot\ldots\cdot g_n(x)+g_1(x)\cdot g_2'(x)\cdot\ldots\cdot g_n(x)+$ $+\ldots+g_1(x)\cdot g_2(x)\cdot\ldots\cdot g_n'(x)$. Ve druhém až $n-tém$ sčítanci je faktor g_1 přímo obsažen a můžeme jej z nich vytknout, proto se blíže zaměříme jen na součin $g_1'(x)\cdot g_2(x)\cdot\ldots\cdot g_n(x)$, který také musí být dělitelný polynomem g_1. Jelikož podle předpokladu platí $D(g_i,\ g_j)=1$, pro všechna $i, j=1,\ 2,\ \ldots,\ n,\ i\neq j$, musí faktor g_1 nutně dělit mnohočlen g_1', který je však derivací g_1, a podle pravidel pro derivování víme, že $st(g_1)>st(g_1')$, z čehož plyne $g_1'=0$ (jinak by nešlo provést dělení polynomu nižšího stupně polynomem stupně vyššího). To pak znamená, že faktor g_1 musí být konstanta, což je ve sporu s předpokladem $st(g_i)\geq 1$, pro $i=1,\ 2,\ \ldots,\ n,$ a tudíž platí původní tvrzení. Tímto je dokázána nutná a postačující podmínka pro rozklad mnohočlenu v součinu faktorů nedělitelných čtvercem.

Věta 5.2.

Nechť $I[x]$ je obor integrity s jednoznačným rozkladem charakteristiky 0 a $f(x)\in I[x]$ je primitivní polynom. Potom $f(x)$ je dělitelný čtvercem právě tehdy, když mnohočleny $f(x)$ a $f'(x)$ nejsou nesoudělné, tj. $D(f(x),\ f'(x))\neq 1$.

Příklad 5.2.

a) Ověřte, zda je polynom $f(x)=x^3+4x^2+5x+2$ dělitelný čtvercem nějakého polynomu v oboru integrity $\mathbb{Z}[x]$.

Řešení:

Tento polynom $f(x)=x^3+4x^2+5x+2$ derivujeme a dostaneme $f'(x)=3x^2+8x+5$. Nyní zjistíme, zda jsou polynomy $f(x)$ a $f'(x)$ soudělné nebo nesoudělné.

$D(f(x),f'(x))=(x+1)\neq 1$, z čehož vidíme, že $f(x)$ a jeho derivace nejsou nesoudělné a mnohočlen $f(x)$ je tedy dělitelný čtvercem polynomu $v(x)=x+1$.

Provedeme-li rozklad polynomu $f(x)$ na kořenové činitele, dostaneme rovnost $f(x)=(x+2)(x+1)^2$, takže náš závěr byl správný a polynom $f(x)$ je skutečně dělitelný čtvercem.

b) Ověřte, zda je polynom $f(x) = x^3 + x^2 - 4x - 4$ dělitelný čtvercem nějakého polynomu v oboru $Z[x]$.

Řešení:

Mnohočlen $f(x)$ derivujeme, $f'(x) = 3x^2 + 2x - 4$, a zjišťujeme soudělnost mnohočlenů $f(x)$ a $f'(x)$. $D(f(x), f'(x)) = 1$, což znamená, že polynomy soudělné nejsou a $f(x)$ tedy není dělitelný čtvercem. Úplný rozklad mnohočlenu zapíšeme $f(x) = x^3 + x^2 - 4x - 4 =$ $= (x+1)(x+2)(x-2)$, ze kterého je dobře vidět, že není existence čtverce dělícího tento mnohočlen.

Nyní přejdeme algoritmu pro rozklad polynomu v oboru integrity $I[x]$ s jednoznačným rozkladem charakteristiky 0 v součin faktorů nedělitelných čtvercem, který pochází od Davida Mussera.

5.2. Musserův algoritmus

Polynom $f(x) \in I[x]$ je primitivní polynom s koeficienty z oboru I. Chceme jej zapsat jako součin faktorů nedělitelných čtvercem, to znamená zapsat jej ve tvaru, kde mnohočleny $f(x) = v_1^1(x) \cdot v_2^2(x) \cdot \ldots \cdot v_k^k(x)$ $v_i \in I[x]$ nejsou dělitelné čtvercem a jsou po dvou nesoudělné ($D(v_i, v_j) = 1$, pro všechna $i, j = 1, 2, \ldots, k, i \neq j$). Prvním krokem řešení je nalezení formální derivace polynomu $f(x)$, tj. $f(x): f'(x) = \left[v_1^1(x) \cdot v_2^2(x) \cdot \ldots \cdot v_k^k(x)\right]' =$ $= v_1'(x) \cdot v_2^2(x) \cdot \ldots \cdot v_k^k(x) + v_1(x) \cdot 2v_2(x) \cdot v_2'(x) \cdot \ldots \cdot v_k^k(x) + \ldots + v_1(x) \cdot v_2^2(x) \cdot \ldots \cdot kv_k^{k-1}(x) v_k'(x)$. Ze všech sčítanců této derivace můžeme maximálně vytknout součin $v_1^0(x) \cdot v_2^1(x) \cdot \ldots \cdot v_k^{k-1}(x)$, který je obsažen i v zápisu mnohočlenu $f(x)$. Zároveň se jedná o největší společný dělitel polynomů $f(x)$ a $f'(x) - D(f(x), f'(x)) = v_1^0(x) \cdot v_2^1(x) \cdot \ldots \cdot v_k^{k-1}(x)$. Nyní zavedeme pomocný polynom $p(x) = \dfrac{f(x)}{D(f(x), f'(x))}$. Mnohočlen $D(f(x), f'(x))$ obsahuje stejné členy $v_i, i = 1, 2, \ldots, k$ jako polynom $f(x)$, ale každý má exponent o 1 menší, z toho vyplývá,

že pomocný polynom $p(x), p(x) = v_1(x) \cdot v_2(x) \cdot \ldots \cdot v_k(x)$, obsahuje všechny faktory v_i a to v první mocnině.

Jestliže spočítáme největší společný dělitel $D\big(p(x), D\big(f(x), f'(x)\big)\big)$, dostaneme $D\big(p(x), D\big(f(x), f'(x)\big)\big) = v_2(x) \cdot \ldots \cdot v_k(x)$. Dosazením tohoto největšího společného dělitele do podílu $\frac{p(x)}{D\big(p(x), D\big(f(x), f'(x)\big)\big)} = \frac{v_1(x) \cdot v_2(x) \cdot \ldots \cdot v_k(x)}{v_2(x) \cdot \ldots \cdot v_k(x)} = v_1(x)$ jsme získali první faktor mnohočlenu $f(x)$.

Zbývající faktory lze zjistit dvěma způsoby. Prvním způsobem můžeme využít druhé derivace $f''(x)$, nebo druhým způsobem dále pracovat s mnohočlenem $D\big(f(x), f'(x)\big)$, kde získáme další faktor $v_2(x)$, který se nachází v první mocnině, místo s polynomem $f(x)$.

Příklad 5.3.

Rozložte mnohočlen $f(x) = x^6 + 10x^5 + 40x^4 + 82x^3 + 91x^2 + 52x + 12$ na součin faktorů nedělitelným čtvercem, $f(x) \in \mathbb{Z}[x]$.

Řešení:

Nejprve podle výše popsaného postupu stanovíme první derivaci polynomu $f(x)$. Dostáváme $f'(x) = 6x^5 + 50x^4 + 160x^3 + 246x^2 + 182x + 52$, nyní zjistíme největší společný dělitel $d_1(x) = D\big(f(x), f'(x)\big) = x^3 + 4x^2 + 5x + 2$. Vypočteme pomocný polynom $p_1(x) = \frac{f(x)}{d_1(x)} = \frac{x^6 + 10x^5 + 40x^4 + 82x^3 + 91x^2 + 52x + 12}{x^3 + 4x^2 + 5x + 2} = x^3 + 6x^2 + 11x + 6$.

Mnohočlen $p_1(x)$ je součinem všech faktorů vyskytujících se v polynomu $f(x)$. Nyní vyčíslíme největší společný dělitel $D\big(p_1(x), d_1(x)\big) = x^2 + 3x + 2$ a dosadíme do podílu $v_1(x) = \frac{p_1(x)}{D\big(p_1(x), d_1(x)\big)} = \frac{x^3 + 6x^2 + 11x + 6}{x^2 + 3x + 2} = x + 3$. Tím získáváme faktor $v_1(x)$, který je v polynomu $f(x)$ první mocnině. Dále budeme pokračovat ve výpočtu zbývajících faktorů. Jak bylo naznačeno v popisu algoritmu pro square-free decomposition, máme dvě možnosti dalšího řešení. Využijeme tu možnost, kde budeme dále pracovat s polynomem

$d_1(x) = D\big(f(x), f'(x)\big) = x^3 + 4x^2 + 5x + 2$, který obsahuje stejné faktory jako $f(x)$, ovšem každý faktor bude mít exponent o jednu menší. Nejprve budeme derivovat $d_1'(x) = \left[x^3 + 4x^2 + 5x + 2\right]' = 3x^2 + 8x + 5$ a použijeme ke zjištění největšího společného dělitele $d_2(x) = D\Big(d_1(x), d_1'(x)\Big) = x + 1$. Nyní spočteme druhý pomocný polynom $p_2(x) = \dfrac{d_1(x)}{d_2(x)} = \dfrac{x^3 + 4x^2 + 5x + 2}{x + 1} = x^2 + 3x + 2$, pomocí něj pak $D\big(p_2(x), d_2(x)\big) = x + 1$ a oba výsledky dosadíme do podílu $v_2(x) = \dfrac{p_2(x)}{D\big(p_2(x), d_2(x)\big)} = \dfrac{x^2 + 3x + 2}{x + 1} = x + 2$, získáme druhý faktor, který má v zadaném polynomu $f(x)$ zastoupení ve druhé mocnině. Zároveň mnohočlen $d_2(x) = x + 1$ je třetím faktorem polynomu $f(x)$ a je v něm zastoupen ve třetí mocnině.

Polynom $f(x)$ jsme rozložili na součin faktorů nedělitelných čtvercem, a proto můžeme psát $f(x) = (x + 3)(x + 2)^2 (x + 1)^3$.

Kontrolu můžeme provést pouhým roznásobením závorek a dostaneme opět původní polynom.

$$f(x) = (x + 3)(x + 2)^2 (x + 1)^3 = x^6 + 10x^5 + 40x^4 + 82x^3 + 91x^2 + 52x + 12 .$$

Tato rovnost skutečně platí.

Příklad 5.4.

Rozložte

$g(x) = x^{10} + x^9 - 33x^8 + 41x^7 + 293x^6 - 993x^5 + 1037x^4 + 131x^3 - 1098x^2 + 820x - 200$, kde $g(x) \in Z[x]$, v součin faktorů nedělitelných čtvercem.

Řešení:

Opět začneme derivováním polynomu $g(x)$, $g'(x) = 10x^9 + 9x^8 - 264x^7 + 287x^6 + +1758x^5 - 4965x^4 + 4148x^3 + 393x^2 - 2196x + 820$ a určením největšího společného dělitele $d_1(x) = D\big(g(x), g'(x)\big) = x^6 - 2x^5 - 16x^4 + 70x^3 - 109x^2 + 76x - 20$. Derivaci i největší společný dělitel dosadíme do podílu a dostaneme pomocný polynom $p_1(x) =$

$= \frac{g(x)}{d_1(x)} = x^4 + 3x^3 - 11x^2 - 3x + 10$, který použijeme ve výpočtu největšího společného dělitele $D\big(p_1(x), d_1(x)\big) = x^3 + 2x^2 - 13x + 10$. Nyní dosadíme do podílu $v_1(x) =$

$= \frac{p_1(x)}{D\big(p_1(x), d_1(x)\big)} = \frac{x^4 + 3x^3 - 11x^2 - 3x + 10}{x^3 + 2x^2 - 13x + 10} = x + 1.$

Získali jsme první faktor, který je v polynomu $g(x)$ obsažen v první mocnině.

Přejdeme k určování druhého faktoru, k čemuž použijeme polynom (společného dělitele) $d_1(x) = D\big(g(x), g'(x)\big) = x^6 - 2x^5 - 16x^4 + 70x^3 - 109x^2 + 76x - 20$, v němž je tento druhý faktor v první mocnině. Spočítáme proto derivaci $d_1'(x) = 6x^5 - 10x^4 -$

$-64x^3 + 210x^2 - 218x + 76$ a přejdeme k společnému děliteli $d_2(x) = D\left(d_1(x), d_1'(x)\right) =$

$= x^3 - 4x^2 + 5x - 2$ a dosadíme do podílu $x^3 + 2x^2 - 13x + 10$. Nyní zjistíme hodnotu největšího společného jmenovatele $D\big(p_2(x), d_2(x)\big) = x^2 - 3x + 2$ a vypočítáme faktor

$v_2(x) = \frac{p_2(x)}{D\big(p_2(x), d_2(x)\big)} = \frac{x^3 + 2x^2 - 13x + 10}{x^2 - 3x + 2} = x + 5.$

Dalším krokem je určování třetího faktoru. Derivujeme polynom $d_2(x) = D\left(d_1(x), d_1'(x)\right) =$

$= x^3 - 4x^2 + 5x - 2$ a dostaneme mnohočlen $d_2'(x) = 3x^2 - 8x + 5$. Hledaný společný dělitel je $d_3(x) = D\left(d_2(x), d_2'(x)\right) = x - 1$ a pomocný mnohočlen $p_3(x) = \frac{d_2(x)}{d_3(x)} = x^2 - 3x + 2$.

Faktor je tedy $v_3(x) = \frac{p_3(x)}{D\big(p_3(x), d_3(x)\big)} = \frac{x^2 - 3x + 2}{x - 1} = x - 2$. V polynomu $g(x)$ je zastoupen ve třetí mocnině.

Přistoupíme k určení čtvrtého faktoru $v_4(x)$, který již nemusíme určovat, neboť je vidět v polynomu $d_3(x) = D\left(d_2(x), d_2'(x)\right) = x - 1$, tudíž $v_4(x) = x - 1$.

Tím jsme ukončili rozklad polynomu $g(x)$ na součin faktorů nedělitelných čtvercem a zapíšeme: $g(x) = (x+1)(x+5)^2(x-2)^3(x-1)^4$.

Zkoušku o správnosti square-free rozkladu se přesvědčíme pouhým roznásobením závorek.

$(x+1)(x+5)^2(x-2)^3(x-1)^4 = x^{10} + x^9 - 33x^8 + 41x^7 + 293x^6 - 993x^5 + 1037x^4 +$
$+ 131x^3 - 1098x^2 + 820x - 200$

Opět jsme ověřili, že tato rovnost platí.

Kromě tohoto algoritmu existují další varianty postupů při rozkladu v součin square-free faktorů, patří mezi ně například Tobeyho-Horowitzův algoritmus nebo Yunův algoritmus, které si také představíme.

5.3. Tobeyho-Horowitzův algoritmus

Nechť polynom $f(x) \in I[x]$ je primitivní polynom s koeficienty z oboru I, přičemž platí $f(x) = v_1^1(x) \cdot v_2^2(x) \cdot \ldots \cdot v_k^k(x)$, kde mnohočleny $v_i \in I[x]$ nejsou dělitelné čtvercem a jsou po dvou nesoudělné ($D(v_i, v_j) = 1$, pro všechna $i, j = 1, 2, \ldots, k, i \neq j$). Postupovat budeme tak, že nejprve spočteme první derivaci polynomu $f'(x)$ a největší společný dělitel $g_1(x) = D(f(x), f'(x)) = v_2(x) \cdot v_3^2(x) \cdot \ldots \cdot v_k^{k-1}(x)$. Pak bude následovat určení podílu, který budeme značit $h_1(x)$, $h_1(x) = \frac{f(x)}{g_1(x)} = v_1(x) \cdot v_2(x) \cdot \ldots \cdot v_k(x)$. V dalším kroku algoritmu musíme spočítat polynom $g_2(x) = D\left(g_1(x), g_1'(x)\right) = v_3(x) \cdot v_4^2(x) \cdot \ldots \cdot v_k^{k-2}(x)$ a polynom $h_2(x) = \frac{g_1(x)}{g_2(x)} = v_2(x) \cdot v_3(x) \cdot \ldots \cdot v_k(x)$. Podíl $\frac{h_1(x)}{h_2(x)} = v_1(x)$ určuje první faktor $f(x)$, ve kterém je zastoupen v první mocnině. Další lineární faktory $v_i, i = 2, \ldots, k,$ zjistíme určením polynomů $g_{i+1}(x) = D\left(g_i(x), g_i'(x)\right) = v_{i+2}(x) \cdot v_{i+3}^2(x) \cdot \ldots \cdot v_k^{k-(i+1)}(x)$ a $h_{i+1}(x) = \frac{g_i(x)}{g_{i+1}(x)} =$

$= v_{i+1}(x) \cdot v_{i+2}(x) \cdot \ldots \cdot v_k(x)$, a podíl $v_i(x) = \frac{h_i(x)}{h_{i+1}(x)}$. Nyní si předvedeme na příkladu uvedený postup.

Příklad 5.5.

Rozložte

$f(x) = x^{10} - 23x^9 + 183x^8 - 307x^7 - 3859x^6 + 23691x^5 - 31331x^4 - 145505x^3 +$

$+ 640350x^2 - 972000x + 540000$, $f(x) \in Z[x]$, v součin faktorů nedělitelných čtvercem.

Řešení: Zadaný polynom $f(x)$ derivujeme a píšeme $f'(x) = 10x^9 - 207x^8 +$ $+1464x^7 - 2149x^6 - 23154x^5 + 118455x^4 - 125324x^3 - 436515x^2 + 1280700x - 972000$.

Nyní spočteme největší společný dělitel $g_1(x) = D(f(x), f'(x)) = x^6 - 17x^5 + 90x^4 - 14x^3$ $-1415x^2 + 4575x - 4500$ a podíl $h_1(x) = \frac{f(x)}{g_1(x)} = x^4 - 6x^3 - 9x^2 + 94x - 120$. Derivujeme mnohočlen $g_1(x)$ a získáváme $g_1'(x) = 6x^5 - 85x^4 + 360x^3 - 42x^2 - 2830x + 4575$. Nyní pokračujeme určením $g_2(x) = D\left(g_1(x), g_1'(x)\right) = x^3 - 13x^2 + 55x - 75$ a $h_2(x) = \frac{g_1(x)}{g_2(x)} =$ $= x^3 - 4x^2 - 17x + 60.$ První faktor polynomu $f(x)$ získáme pomocí podílu $v_1(x) = \frac{h_1(x)}{h_2(x)} = \frac{x^4 - 6x^3 - 9x^2 + 94x - 120}{x^3 - 4x^2 - 17x + 60} = x - 2$ a je obsažen v první mocnině.

Pokračujeme výpočtem mnohočlenu $g_3(x) = D\left(g_2(x), g_2'(x)\right) = x - 5$ a $h_3(x) = \frac{g_2(x)}{g_3(x)} =$ $\frac{x^3 - 13x^2 + 55x - 75}{x - 5} = = x^2 - 8x + 15.$ Podílem získáme druhý faktor, $v_2(x) = \frac{h_2(x)}{h_3(x)} =$ $\frac{x^3 - 4x^2 - 17x + 60}{x^2 - 8x + 15} = x + 4.$ Druhý činitel $v_2(x) = x + 4$ se vyskytuje v polynomu $f(x)$ ve druhé mocnině. Pokračujeme

k zjištění $g_4(x) = D\left(g_3(x), g_3'(x)\right) = 1$ a $h_4(x) = \frac{g_3(x)}{g_4(x)} = \frac{x - 5}{1} = x - 5$. Třetí faktor $v_3(x) = \frac{h_3(x)}{h_4(x)} = \frac{x^2 - 8x + 15}{x - 5} = x - 3$ je v polynomu $f(x)$ ve třetí mocnině a posledním faktorem $v_4(x) = h_4(x) = x - 5$, kde se faktor nachází v polynomu $f(x)$ ve čtvrté mocnině.

Tím jsme ukončili rozklad a můžeme napsat: $f(x) = (x-2)(x+4)^2(x-3)^3(x-5)^4$.

O správnosti dosaženého výsledku se přesvědčíme roznásobením:

$(x-2)(x+4)^2(x-3)^3(x-5)^4 = x^{10} - 23x^9 + 183x^8 - 307x^7 - 3859x^6 + 23691x^5 -$
$-31331x^4 - 145505x^3 + 640350x^2 - 972000x + 540000.$

Získali jsme, že rovnost platí.

5.4. Yunův algoritmus

Buď $f(x) \in I[x]$ primitivní polynom s koeficienty z oboru I, přičemž platí $f(x) = v_1^1(x) \cdot v_2^2(x) \cdot \ldots \cdot v_k^k(x)$, kde mnohočleny $v_i \in I[x]$ nejsou dělitelné čtvercem a jsou po dvou nesoudělné ($D(v_i, v_j) = 1$, pro všechna $i, j = 1, 2, \ldots, k, i \neq j$). Derivujeme mnohočlen $f(x)$ a získáme polynom $f'(x)$. Spočteme-li nyní největší společný dělitel, dostaneme polynom $u(x) = D(f(x), f'(x)) = v_2(x) \cdot v_3^2(x) \cdot \ldots \cdot v_k^{k-1}(x)$, který obsahuje všechny faktory polynomu $f(x)$, ale každý s exponentem zmenšeným o jedna. Následuje výpočet podílů $g_1(x) = \frac{f(x)}{u(x)}$ a $h_1(x) = \frac{f'(x)}{u(x)}$ konečně polynom $v_1(x) =$ $= D\left(g_1(x), h_1(x) - g_1'(x)\right)$, který je prvním faktorem mnohočlenu $f(x)$ vyskytujícím se v něm v první mocnině. Pro výpočet dalších faktorů v_i, $i = 2, \ldots, k$, pak již stačí počítat polynomy $g_i(x) = \frac{g_{i-1}(x)}{v_{i-1}(x)}$ a $h_i(x) = \frac{h_{i-1} - g_{i-1}'(x)}{v(x)}$ a jako poslední největšího společného dělitele. Tento postup si opět ukážeme v následujícím příkladě.

Příklad 5.6.

Rozložte: $f(x) = x^{10} - 25x^8 + 10x^7 + 195x^6 - 124x^5 - 575x^4 + 570x^3 + 500x^2 - 840x + 288$, $f(x) \in Z[x]$, v součin faktorů nedělitelných čtvercem.

Řešení:

Nejprve vyjádříme derivaci

$$f'(x) = 10x^9 - 200x^7 + 70x^6 + 1170x^5 - 620x^4 - 2300x^3 + 1710x^2 + 1000x - 840,$$

a určíme největšího společného dělitele:

$$u(x) = D(f(x), f'(x)) = x^6 - 2x^5 - 8x^4 + 14x^3 + 11x^2 - 28x + 12.$$

Dosadíme do podílů:

$g_1(x)=\frac{f(x)}{u(x)}=x^4+2x^3-13x^2-14x+24$ a $h_1(x)=\frac{f'(x)}{u(x)}=10x^3+20x^2-80x-70$.

Nyní nalezneme $D\left(g_1(x),h_1(x)-g_1'(x)\right)$, dostáváme první faktor $v_1(x)=x+4$, který je zastoupený v polynomu $f(x)$ první mocninou.

Než budeme moci vypočítat druhý faktor $v_2(x)$, musíme nejprve zjistit mnohočlen $g_2(x)$ jako podíl $\frac{g_1(x)}{v_1(x)}=\frac{x^4+2x^3-13x^2-14x+24}{x+4}=x^3-2x^2-5x+6$ a druhý mnohočlen $h_2(x)=\frac{h_1-g_1'(x)}{v_1(x)}=\frac{6x^3+14x^2-54x-56}{x+4}=6x^2-10x-14$. Nyní musí následovat určení největšího společného dělitele $D\left(g_2(x),h_2(x)-g_2'(x)\right)=v_2(x)=x-3$ a dostáváme druhý faktor polynomu $f(x)$, který je zastoupený druhou mocninou. Pro třetí faktor opět počítáme mnohočleny $g_3(x)=\frac{g_2(x)}{v_2(x)}=\frac{x^3-2x^2-5x+6}{x-3}=x^2+x-2$ a $h_3(x)=\frac{h_2-g_2'(x)}{v_2(x)}=$

$=\frac{3x^2-6x-9}{x-3}=3x+3$, bez nichž nevyjádříme faktor $v_3(x)=D\left(g_3(x),h_3(x)-g_3'(x)\right)=$

$=x+2$, jenž se v $f(x)$ nachází ve třetí mocnině. Čtvrtý faktor $v_4(x)$ dostaneme dopočtením mnohočlenů $g_4(x)=\frac{g_3(x)}{v_3(x)}=\frac{x^2+x-2}{x+2}=x-1$ a $h_4(x)=\frac{h_3-g_3'(x)}{v_3(x)}=\frac{x+2}{x+2}=1$. Pokud spočítáme derivaci $g_4'(x)=1$ a po odečtení derivace od $h_4(x)$, resp. $h_4(x)-g_4'(x)$, dostaneme rozdíl roven nule. Hledaný největší společný dělitel a zároveň čtvrtý faktor, můžeme psát, že $v_4(x)=D\left(g_4(x),\ h_4(x)-g_4'(x)\right)=D(x-1,\ 0)=x-1$. Těmito kroky jsme získali všechny faktory, které se vyskytují v daném polynomu $f(x)$, a proto ho můžeme zapsat ve tvaru $f(x)=(x+4)(x-3)^2(x+2)^3(x-1)^4$.

O kontrole správnosti rozkladu nalezeného square-free se přesvědčíme opět roznásobením: $(x+4)(x-3)^2(x+2)^3(x-1)^4=x^{10}-25x^8+10x^7+195x^6-124x^5-575x^4+570x^3+500x^2-$ $-840x+288$.

Poznámka: *Tobeyho-Horowitzův* a *Yunův* algoritmus na rozdíl od *Musserova* algoritmu je mnohem výhodnější díky počítání jen jednoho největšího společného dělitele v každém kroku. Tento krok není zrovna jednoduchou záležitostí oproti zjištění první derivace či podílu mnohočlenů. Tato skutečnost pak nabývá na důležitosti zvláště při faktorizaci polynomů vyšších stupňů.

Při hledání největšího společného dělitele dvou polynomů byl velkou oporou program počítačové algebry *Wolfram Mathematica*®.

Šestá kapitola

6.1. Ukázky výpočtů v prostředí *Wolfram Mathematica 8*®

V dnešní době již máme k dispozici několik počítačových programů, které mohou za velmi krátkou dobu provést náročnější početní operace. Mezi přední světové programy v současnosti patří *Wolfram Mathematica*® a *Maple*®. Příjemné prostředí nabízí *Wolfram Mathematica 8*® – využijme této skutečnosti a pokusme se zjistit, kam až sahá výkon jádra tohoto programu. Příklady rozkladů polynomů, kterými jsme se již zabývali v této práci (nepoužili jsme přitom žádný počítačový algebraický systém), je tento program schopen vyřešit za dobu velmi krátkou. Zajímavější ovšem bude sestavit natolik komplikované polynomy, jejichž rozklad v součin bude trvat až několik sekund. Tento požadavek patrně není jednoduché splnit, proto postupujme „opačně“. Předem si sestavíme výsledek (již hotový součin), ke kterému se máme dopracovat. Tento součin upravíme (roznásobíme všechny závorky). Takto získaný polynom se opět pokusíme rozložit v součin, přičemž budeme sledovat dobu potřebnou k tomuto rozkladu.

Příklad 1

Definujme do paměti polynom

$$r(x)=(-302x^7+3)(401x^3-6)(506x^{15}+8)(-5x^4+4)(-7x^7+4)^7(-4x^3+5)^{16}(3x^5-2)^{17}(-9x^{12}+7)^{14}$$

```
In[1]:= r[x_] := (-302 x^16 + 3) (401 x^15 - 6) (506 x^13 + 8) (-5 x^4 + 4)
          (-7 x^7 + 4)^7 (-4 x^3 + 5)^16 (3 x^5 - 2)^17 (-9 x^12 + 7)^14
```

Dále do paměti definujme polynom $s(x)$, který vznikne roznásobením závorek výše.

```
In[2]:= s[x_] := Expand[r[x]]
```

Samozřejmě bychom mohli polynom $s(x)$ nechat zobrazit na obrazovce, ale to by nemělo pro nás žádný význam – zabrali bychom zde mnoho místa. Nyní se pokusíme tento polynom opět rozložit v součin, tj. v součin, který představuje polynom $r(x)$. Budeme přitom měřit potřebný čas k provedení této operace.

```
In[3]:= mereni = Timing[Factor[s[x]]]
Out[3]= {0.23, -2 (-5 + 4 x^3)^16 (-4 + 5 x^4) (-2 + 3 x^5)^17 (-4 + 7 x^7)^7
          (-7 + 9 x^12)^14 (4 + 253 x^13) (-6 + 401 x^15) (-3 + 302 x^16)}
```

Obdrželi jsme vektor, jehož první složkou je číslo $0,23$ a druhou složkou je polynom $r(x)$, tedy polynom $s(x)$ po faktorizaci. Provedení faktorizace tedy trvalo $0,23$ sekund, což je ukazatelem velmi výkonného jádra programu – uvažme, že polynom $s(x)$ je velmi komplikovaný, jeho stupeň činní 398 a vedoucí koeficient u nejvyšší mocniny neznámé x činní $3201654325830802551805454200658171359647498240$.

Příklad 2

Definujme do paměti polynom

$$f(x)=\prod_{a=1}^{100}(4x-5a)=(4x-5)(4x-10)\cdot\ldots\cdot(4x-500).$$

```
In[5]:= f[x_] := Product[-5 a + 4 x, {a, 1, 100}]
```

Dále do paměti definujme polynom $g(x)$, který vznikne roznásobením závorek výše.

```
In[6]:= g[x_] := Expand[f[x]]
```

Nyní se pokusíme tento polynom opět rozložit v součin, tj. v součin, který představuje polynom $f(x)$. Opět měřme potřebný čas k provedení této operace.

```
In[7]:= mereni2 = Timing[Factor[g[x]]];
```

Za příkazem výše jsme použili středník – to proto, aby se polynom nezobrazoval. Dále opět bychom obdrželi vektor, jehož první složkou je hledaný čas a druhou složkou je polynom $f(x)$. Zajímá nás pouze hledaný čas, proto zobrazme jen první složku tohoto vektoru.

```
In[8]:= First[mereni2]

Out[8]= 0.361
```

Potřebný čas k provedení faktorizace byl tedy $0,361$ sekund.

Příklad 3

Postupujme analogicky jako v předchozích příkladech.

Definujme polynom

$$b(x)=\prod_{a=1}^{100}\left(7x^2+30x+a\right)=(7x^2+30x+1)(7x^2+30x+2)\cdot\ldots\cdot(7x^2+30x+100)\,.$$

```
In[9]:= b[x_] := Product[a + 30 x + 7 x^2, {a, 1, 100}]
```

Dále definujme polynom $c(x)$, který vznikne roznásobením závorek výše.

```
In[10]:= c[x_] := Expand[b[x]]
```

Změříme potřebný čas.

```
In[11]:= mereni3 = Timing[Factor[c[x]]];

In[12]:= First[mereni3]

Out[12]= 19.037
```

Zde zjišťujeme zajímavější výsledek – potřebná doba činila $19,037$ sekund. Polynom, který byl faktorizován je stupně 200 a číslo, které představuje jeho vedoucí koeficient, má 85 cifer.

Příklad 4

Definujme polynom

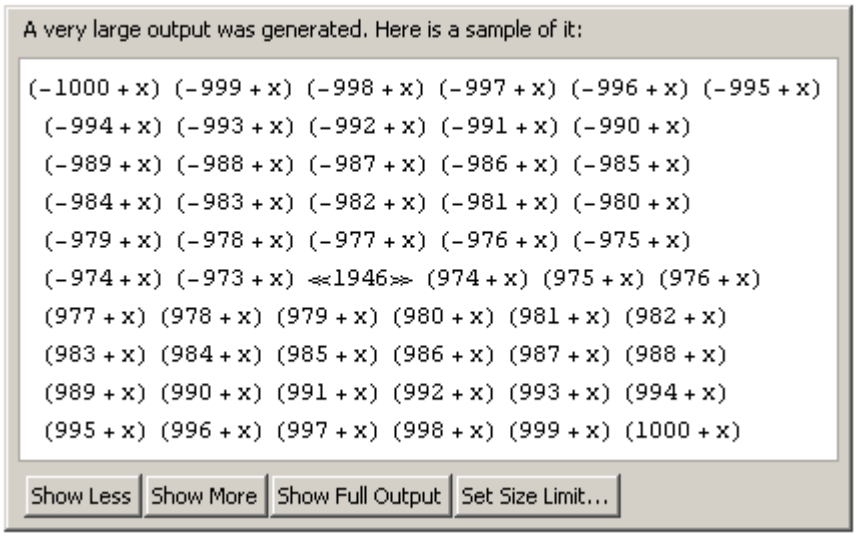
$$h(x)=\prod_{a=-1000}^{1000}\left(x+a\right)=(x-1000)(x-999)\cdot\ldots\cdot(x-1)x(x+1)\cdot\ldots\cdot(x+1000)\,.$$

```
In[13]:= h[x_] := Product[a + x, {a, -1000, 1000}]
```

Zvědavost nás může vést k otázce, jak *Mathematica* zobrazuje „velmi dlouhé“ výrazy.

Pokusme se zobrazit polynom $h(x)$:

```
In[14]:= h[x]
```

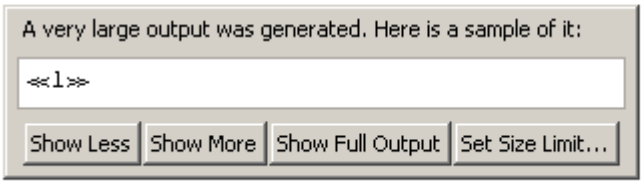


Je vidět, že prostředí *Mathematica* bylo velmi dobře propracováno svými tvůrci i po grafické stránce.

Dále definujme polynom $j(x)$, který vznikne roznásobením závorek výše.

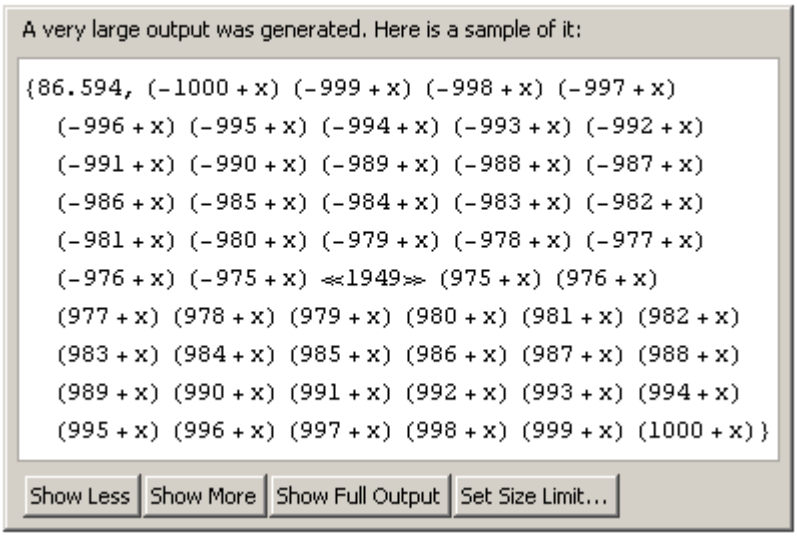
```
In[15]:= j[x_] := Expand[h[x]]
```

```
In[16]:= j[x]
```



Změřme potřebný čas.

```
In[17]:= Timing[Factor[j[x]]]
```



Hledaný čas je zobrazen v tabulce vlevo nahoře a činí $86,594$ sekund. Tento výsledek je již zajímavější, k provedení operace bylo potřeba více než jedna minuta. Faktorizovali jsme polynom stupně 2001, jehož vedoucí koeficient je ovšem roven jedné. Uvedené výsledky jsou vskutku fascinující a jsou výsledkem pokroku, který nejprve připravili matematici a v posledních letech zdokonalili softwaroví specialisté. Je poctivé říci, že „hlavním motorem" nemůže být postup, který jsme pod vlivem tradice označili jako Kroneckerův algoritmus, ačkoli byl asi znám dříve.

Nahlédli jsme, že v tomto algoritmu s rostoucím stupněm polynomu velice rychle narůstá množina zkoumaných případů a s ní i nároky na využitou paměť i čas výpočtu. Jde však o algoritmus relativně jednoduchý po stránce programování. Proto je asi využit v kalkulátorech třídy TI-92 Plus, ale pro polynomy vyšších stupňů selže.

Také algoritmy pro „bezčtvercový" rozklad polynomu mohou mít jen pomocný význam. Skutečným „motorem" stojícím za shora uvedenými výsledky jsou tzv. modulární algoritmy, nehledající rozklad polynomu $f(x)$ v $\mathbb{Z}[x]$, ale jeho obrazu $\tilde{f}(x)$ v oboru integrity $\mathbb{Z}_p[x]$, p – prvočíslo. Takovýto rozklad by měl být snáze k nalezení s přihlédnutím k faktu, že zatímco v $\mathbb{Z}_p[x]$ existuje nekonečně mnoho ireducibilních polynomů daného stupně *n*, je takovýchto polynomů v $\mathbb{Z}_p[x]$ jen konečně mnoho.

Studiu rozkladů polynomů $\tilde{f}(x) \in \mathbb{Z}_p[x]$ se jm. věnovali K. Petr a zejména excelentní slovenský matematik Š. Schwarz a ovšem i mnozí matematici zahraniční. Až příslušný rozklad polynomu $\tilde{f}(x)$ nalezneme (a koeficienty tohoto polynomu jsou z tělesa zbytkových tříd modulo *p*, tj. 0, 1, …, *p*), vznikne otázka, jak se vrátit k původnímu polynomu $f(x) \in \mathbb{Z}[x]$ a získat jeho rozklad. Nyní jsou k dispozici i sofistikované techniky pro tento návrat (Henselovo zdvižení aj.). Studium těchto otázek je ale nad možnosti této bakalářské práce.

Závěrem k příkladům $1-4$ je nutné dodat, že hledané doby k provedení daných operací jsou variabilní. Jejich variabilita je dána samozřejmě hardwarovou konfigurací daného počítače, dále také tím, do jaké míry je jádro programu zatíženo. Pokud provedeme daný výpočet podruhé, doba výpočtu se změní (zpravidla se zkracuje). Nelze proto generalizovat naše výsledky příkladů $1-4$, ale samozřejmě je možno tvrdit, že pro školní účely je prostředí *Mathematica* naprosto dostačující.

6.2. Rozklad polynomů pomocí algoritmů (Musserův, Tobeyho-Horowitzův, Yunnův) v prostředí *Wolfram Mathematica* 8®

Příklad 1

Faktorizujme polynom

$$f(x) = 24883200 + 231828480x + 980529408x^2 + 2483558208x^3 + 4176902400x^4 +$$
$$+ 4870671664x^5 + 3960852368x^6 + 2154277164x^7 + 651473576x^8 - 20026991x^9 -$$
$$-115503204x^{10} - 48316946x^{11} - 5617708x^{12} + 2490015x^{13} + 1096136x^{14} + 115552x^{15} -$$
$$-27408x^{16} - 9089x^{17} - 628x^{18} + 102x^{19} + 20x^{20} + x^{21}$$

Musserovým algoritmem. Použijme program *Mathematica 8®* .

Definujeme polynom $f(x)$ do paměti.

```
In[1]:= f[x_] := 24 883 200 + 231 828 480 x + 980 529 408 x^2 + 2 483 558 208 x^3 +
          4 176 902 400 x^4 + 4 870 671 664 x^5 + 3 960 852 368 x^6 +
          2 154 277 164 x^7 + 651 473 576 x^8 - 20 026 991 x^9 - 115 503 204 x^10 -
          48 316 946 x^11 - 5 617 708 x^12 + 2 490 015 x^13 + 1 096 136 x^14 +
          115 552 x^15 - 27 408 x^16 - 9089 x^17 - 628 x^18 + 102 x^19 + 20 x^20 + x^21
```

Vypočteme první derivaci polynomu $f(x)$.

```
In[2]:= D[f[x], x]

Out[2]= 231 828 480 + 1 961 058 816 x + 7 450 674 624 x^2 + 16 707 609 600 x^3 +
        24 353 358 320 x^4 + 23 765 114 208 x^5 + 15 079 940 148 x^6 +
        5 211 788 608 x^7 - 180 242 919 x^8 - 1 155 032 040 x^9 - 531 486 406 x^10 -
        67 412 496 x^11 + 32 370 195 x^12 + 15 345 904 x^13 + 1 733 280 x^14 -
        438 528 x^15 - 154 513 x^16 - 11 304 x^17 + 1938 x^18 + 400 x^19 + 21 x^20
```

Definujeme polynom $d_1(x) = D(f(x), f'(x))$ a výsledek zobrazme.

```
In[3]:= d1 := PolynomialGCD[f[x], D[f[x], x]]

In[4]:= d1

Out[4]= 34 560 + 266 112 x + 912 240 x^2 + 1 829 360 x^3 + 2 365 496 x^4 +
        2 038 408 x^5 + 1 151 015 x^6 + 379 429 x^7 + 30 248 x^8 - 32 160 x^9 -
        14 786 x^10 - 2302 x^11 + 184 x^12 + 128 x^13 + 19 x^14 + x^15
```

Dále definujme pomocný polynom $p_1(x) = \frac{f(x)}{d_1(x)}$ a tento ještě úpravami zjednodušme.

```
In[5]:= p1 := f[x] / d1

In[6]:= Simplify[p1]

Out[6]= 720 + 1164 x + 404 x^2 - 85 x^3 - 45 x^4 + x^5 + x^6
```

Vypočteme $D\left(p_1(x),\, d_1(x)\right)$.

```
In[7]:= PolynomialGCD[p1, d1]

Out[7]= (-4 + x) (1 + x) (2 + x) (3 + x) (5 + x)
```

Nakonec obdržíme hledaný polynom $v_1(x) = \dfrac{p_1(x)}{D\left(p_1(x),\, d_1(x)\right)}$.

```
In[8]:= v1 = Simplify[p1 / PolynomialGCD[p1, d1]]

Out[8]= -6 + x
```

Další postup je zcela analogický předchozímu, proto jej uveďme již bez komentářů.

```
In[10]:= p2 = D[d1, x]

Out[10]= 266 112 + 1 824 480 x + 5 488 080 x^2 + 9 461 984 x^3 + 10 192 040 x^4 +
          6 906 090 x^5 + 2 656 003 x^6 + 241 984 x^7 - 289 440 x^8 -
          147 860 x^9 - 25 322 x^10 + 2208 x^11 + 1664 x^12 + 266 x^13 + 15 x^14

In[11]:= d2 = PolynomialGCD[d1, D[d1, x]]

Out[11]= -288 - 1704 x - 4316 x^2 - 6078 x^3 -
          5143 x^4 - 2592 x^5 - 669 x^6 - 6 x^7 + 47 x^8 + 12 x^9 + x^10

In[12]:= p2 = Simplify[d1 / d2]

Out[12]= -120 - 214 x - 103 x^2 - 3 x^3 + 7 x^4 + x^5

In[13]:= v2 = Simplify[p2 / PolynomialGCD[p2, d2]]

Out[13]= 5 + x

In[14]:= p3 = D[d2, x]

Out[14]= -1704 - 8632 x - 18 234 x^2 - 20 572 x^3 -
          12 960 x^4 - 4014 x^5 - 42 x^6 + 376 x^7 + 108 x^8 + 10 x^9

In[15]:= d3 = PolynomialGCD[d2, D[d2, x]]

Out[15]= 12 + 52 x + 91 x^2 + 82 x^3 + 40 x^4 + 10 x^5 + x^6

In[16]:= p3 = Simplify[d2 / d3]

In[17]:= v3 = Simplify[p3 / PolynomialGCD[p3, d3]]

Out[17]= -4 + x
```

```
In[18]:= p4 = D[d3, x]
Out[18]= 52 + 182 x + 246 x^2 + 160 x^3 + 50 x^4 + 6 x^5

In[19]:= d4 = PolynomialGCD[d3, D[d3, x]]
Out[19]= 2 + 5 x + 4 x^2 + x^3

In[20]:= p4 = Simplify[d3/d4]
Out[20]= 6 + 11 x + 6 x^2 + x^3

In[21]:= v4 = Simplify[p4/PolynomialGCD[p4, d4]]
Out[21]= 3 + x

In[22]:= p5 = D[d4, x]
Out[22]= 5 + 8 x + 3 x^2

In[23]:= d5 = PolynomialGCD[d4, D[d4, x]]
Out[23]= 1 + x

In[24]:= p5 = Simplify[d4/d5]
Out[24]= 2 + 3 x + x^2

In[25]:= v5 = Simplify[p5/PolynomialGCD[p5, d5]]
Out[25]= 2 + x

In[26]:= p6 = D[d5, x]
Out[26]= 1

In[27]:= d6 = PolynomialGCD[d5, D[d5, x]]
Out[27]= 1

In[28]:= p6 = Simplify[d5/d6]
Out[28]= 1 + x

In[29]:= v6 = Simplify[p6/PolynomialGCD[p6, d6]]
Out[29]= 1 + x
```

Zde algoritmus končí, neboť jsme nalezli takové $i \in \mathbb{N}$, kde $p_i(x) = 1$. Je totiž $p_6(x) = 1$. Dále tedy můžeme zobrazit podobu polynomu $f(x)$ po faktorizaci.

```
In[30]:= v1 * v2^2 * v2^3 * v4^4 * v5^5 * v6^6

Out[30]= (-6 + x) (1 + x)^6 (2 + x)^5 (3 + x)^4 (5 + x)^5
```

Závěrem je možno provést zkoušku (není však povinná).

```
In[31]:= Expand[%]

Out[31]= -48 600 000 - 518 400 000 x - 2 572 290 000 x^2 -
         7 887 258 000 x^3 - 16 743 105 300 x^4 - 26 123 902 952 x^5 -
         31 038 458 611 x^6 - 28 698 247 401 x^7 - 20 913 542 443 x^8 -
         12 080 338 769 x^9 - 5 524 663 359 x^10 - 1 980 969 197 x^11 -
         543 630 319 x^12 - 107 764 917 x^13 - 12 832 921 x^14 + 80 965 x^15 +
         405 375 x^16 + 93 997 x^17 + 12 251 x^18 + 993 x^19 + 47 x^20 + x^21
```

Příklad 2

Faktorizujme polynom

$$f(x) = 339880181760 - 1352237580288x + 1667378184192x^2 - 81051385856x^3 - \\ - 1128424660992x^4 + 331553703936x^5 + 404003929088x^6 - 102305483520x^7 - \\ - 102037439760x^8 + 6640003580x^9 + 15747372240x^{10} + 2125896159x^{11} - \\ - 923881636x^{12} - 326440467x^{13} - 26731104x^{14} + 3574502x^{15} + 749640x^{16} + \\ + 14214x^{17} - 5392x^{18} - 309x^{19} + 12x^{20} + x^{21}$$

Tobeyho-Horowitzovým algoritmem. Použijme program *Mathematica 8®* .

Definujeme polynom $f(x)$ do paměti.

```
In[1]:= f[x_] := 339 880 181 760 - 1 352 237 580 288 x + 1 667 378 184 192 x^2 -
         81 051 385 856 x^3 - 1 128 424 660 992 x^4 + 331 553 703 936 x^5 +
         404 003 929 088 x^6 - 102 305 483 520 x^7 - 102 037 439 760 x^8 +
         6 640 003 580 x^9 + 15 747 372 240 x^10 + 2 125 896 159 x^11 -
         923 881 636 x^12 - 326 440 467 x^13 - 26 731 104 x^14 + 3 574 502 x^15 +
         749 640 x^16 + 14 214 x^17 - 5392 x^18 - 309 x^19 + 12 x^20 + x^21
```

Vypočteme první derivaci polynomu $f(x)$.

```
In[2]:= D[f[x], x]

Out[2]= -1 352 237 580 288 + 3 334 756 368 384 x - 243 154 157 568 x^2 -
         4 513 698 643 968 x^3 + 1 657 768 519 680 x^4 + 2 424 023 574 528 x^5 -
         716 138 384 640 x^6 - 816 299 518 080 x^7 + 59 760 032 220 x^8 +
         157 473 722 400 x^9 + 23 384 857 749 x^10 - 11 086 579 632 x^11 -
         4 243 726 071 x^12 - 374 235 456 x^13 + 53 617 530 x^14 +
         11 994 240 x^15 + 241 638 x^16 - 97 056 x^17 - 5871 x^18 + 240 x^19 + 21 x^20
```

Definujeme polynom $g_1(x) = D\left(f(x), f'(x)\right)$.

```
In[3]:= g1 = PolynomialGCD[f[x], D[f[x], x]]

Out[3]= -101 154 816 + 302 260 224 x - 217 032 704 x^2 -
        114 886 144 x^3 + 135 485 568 x^4 + 35 527 520 x^5 -
        32 473 016 x^6 - 11 545 410 x^7 + 2 051 445 x^8 + 1 536 621 x^9 +
        235 545 x^10 - 1283 x^11 - 3361 x^12 - 201 x^13 + 11 x^14 + x^15
```

Dále je potřeba nalézt polynom $h_1(x) = \frac{f(x)}{g_1(x)}$, výsledek rovnou upravme.

```
In[4]:= h1 = Simplify[f[x]/g1]

Out[4]= -3360 + 3328 x + 670 x^2 - 521 x^3 - 119 x^4 + x^5 + x^6
```

Definujeme polynom $g_2(x) = D\left(g_1(x), g_1'(x)\right)$.

```
In[5]:= g2 = PolynomialGCD[g1, D[g1, x]]

Out[5]= 150 528 - 270 592 x - 4992 x^2 + 153 312 x^3 + 20 060 x^4 -
        32 349 x^5 - 13 923 x^6 - 2018 x^7 - 42 x^8 + 15 x^9 + x^10
```

Dále nalézáme polynom $h_2(x) = \frac{g_1(x)}{g_2(x)}$, výsledek ihned upravme.

```
In[6]:= h2 = Simplify[g1/g2]

Out[6]= -672 + 800 x - 26 x^2 - 99 x^3 - 4 x^4 + x^5
```

Prvním faktorem polynomu $f(x)$ je polynom $v_1(x) = \frac{h_1(x)}{h_2(x)}$, který je obsažen v první mocnině. Tento faktor ihned upravme.

```
In[7]:= v1 = Simplify[h1/h2]

Out[7]= 5 + x
```

Algoritmus samozřejmě bude ještě pokračovat dále. Sled příkazů je zcela analogický sledu předchozímu.

```
In[8]:= g3 = PolynomialGCD[g2, D[g2, x]]

Out[8]= 448 - 496 x - 220 x^2 + 155 x^3 + 95 x^4 + 17 x^5 + x^6

In[9]:= h3 = Simplify[g2/g3]

Out[9]= 336 - 232 x - 103 x^2 - 2 x^3 + x^4
```

In[10]:= $v2 = \text{Simplify}\left[\frac{h2}{h3}\right]$

Out[10]= $-2 + x$

In[11]:= $g4 = \text{PolynomialGCD}[g3, D[g3, x]]$

Out[11]= $-16 + 8x + 7x^2 + x^3$

In[12]:= $h4 = \text{Simplify}\left[\frac{g3}{g4}\right]$

Out[12]= $-28 + 17x + 10x^2 + x^3$

In[13]:= $v3 = \text{Simplify}\left[\frac{h3}{h4}\right]$

Out[13]= $-12 + x$

In[14]:= $g5 = \text{PolynomialGCD}[g4, D[g4, x]]$

Out[14]= $4 + x$

In[15]:= $h5 = \text{Simplify}\left[\frac{g4}{g5}\right]$

Out[15]= $-4 + 3x + x^2$

In[16]:= $v4 = \text{Simplify}\left[\frac{h4}{h5}\right]$

Out[16]= $7 + x$

In[17]:= $g6 = \text{PolynomialGCD}[g5, D[g5, x]]$

Out[17]= 1

In[18]:= $h6 = \text{Simplify}\left[\frac{g5}{g6}\right]$

Out[18]= $4 + x$

In[19]:= $v5 = \text{Simplify}\left[\frac{h5}{h6}\right]$

Out[19]= $-1 + x$

In[20]:= $g7 = \text{PolynomialGCD}[g6, D[g6, x]]$

Out[20]= 1

In[21]:= $h7 = \text{Simplify}\left[\frac{g6}{g7}\right]$

Out[21]= 1

In[22]:= $v6 = \text{Simplify}\left[\frac{h6}{h7}\right]$

Out[22]= $4 + x$

Posledním faktorem je tedy polynom $v_6(x)$, který je obsažen v šesté mocnině. Polynom $f(x)$ po faktorizaci má tedy následující podobu.

```
In[23]:= v1 * v2^2 * v3^3 * v4^4 * v5^5 * v6^6

Out[23]= (-12 + x)^3 (-2 + x)^2 (-1 + x)^5 (4 + x)^6 (5 + x) (7 + x)^4
```

Závěrem je opět možné provést zkoušku, zda jsme provedli faktorizaci správně.

```
In[24]:= Expand[%]

Out[24]= 339 880 181 760 - 1 352 237 580 288 x + 1 667 378 184 192 x^2 -
         81 051 385 856 x^3 - 1 128 424 660 992 x^4 + 331 553 703 936 x^5 +
         404 003 929 088 x^6 - 102 305 483 520 x^7 - 102 037 439 760 x^8 +
         6 640 003 580 x^9 + 15 747 372 240 x^10 + 2 125 896 159 x^11 -
         923 881 636 x^12 - 326 440 467 x^13 - 26 731 104 x^14 + 3 574 502 x^15 +
         749 640 x^16 + 14 214 x^17 - 5392 x^18 - 309 x^19 + 12 x^20 + x^21
```

Příklad 3

Faktorizujme polynom

$$f(x) = 960180480 - 4837480704x + 9203362560x^2 - 6897073536x^3 - 1161139104x^4 +$$
$$+ 4847439168x^5 - 1738450416x^6 - 1118110120x^7 + 774661937x^8 + 105626333x^9 -$$
$$- 154605506x^{10} - 796202x^{11} + 18192715x^{12} - 542745x^{13} - 1348380x^{14} + 23100x^{15} +$$
$$+ 60791x^{16} + 1115x^{17} - 1426x^{18} - 74x^{19} + 13x^{20} + x^{21}$$

Yunnovým algoritmem. Použijme program *Mathematica 8®* .

Definujeme polynom $f(x)$ do paměti.

```
In[1]:= f[x_] := 960 180 480 - 4 837 480 704 x + 9 203 362 560 x^2 -
          6 897 073 536 x^3 - 1 161 139 104 x^4 + 4 847 439 168 x^5 - 1 738 450 416 x^6 -
          1 118 110 120 x^7 + 774 661 937 x^8 + 105 626 333 x^9 - 154 605 506 x^10 -
          796 202 x^11 + 18 192 715 x^12 - 542 745 x^13 - 1 348 380 x^14 +
          23 100 x^15 + 60 791 x^16 + 1115 x^17 - 1426 x^18 - 74 x^19 + 13 x^20 + x^21
```

Vypočteme první derivaci tohoto polynomu.

```
In[2]:= D[f[x], x]

Out[2]= -4 837 480 704 + 18 406 725 120 x - 20 691 220 608 x^2 - 4 644 556 416 x^3 +
        24 237 195 840 x^4 - 10 430 702 496 x^5 - 7 826 770 840 x^6 +
        6 197 295 496 x^7 + 950 636 997 x^8 - 1 546 055 060 x^9 - 8 758 222 x^10 +
        218 312 580 x^11 - 7 055 685 x^12 - 18 877 320 x^13 + 346 500 x^14 +
        972 656 x^15 + 18 955 x^16 - 25 668 x^17 - 1406 x^18 + 260 x^19 + 21 x^20
```

Definujeme polynom $u(x) = D(f(x), f'(x))$.

```
In[3]:= u = PolynomialGCD[f[x], D[f[x], x]]

Out[3]= -762048 + 3084480 x - 4427568 x^2 + 1959408 x^3 +
        1250076 x^4 - 1397164 x^5 + 74687 x^6 + 303129 x^7 - 62140 x^8 -
        32692 x^9 + 8322 x^10 + 2014 x^11 - 440 x^12 - 72 x^13 + 7 x^14 + x^15
```

Následuje výpočet polynomu $g_1(x) = \frac{f(x)}{u(x)}$ a samozřejmě jeho úprava.

```
In[4]:= g1 = Simplify[f[x]/u]

Out[4]= -1260 + 1248 x + 295 x^2 - 246 x^3 - 44 x^4 + 6 x^5 + x^6
```

Dále nalézáme polynom $h_1(x) = \frac{D(f(x),\, f'(x))}{u(x)}$ a opět provádíme drobné úpravy.

```
In[5]:= h1 = Simplify[D[f[x], x]/u]

Out[5]= 6348 + 1540 x - 3497 x^2 - 685 x^3 + 113 x^4 + 21 x^5
```

Nakonec nalézáme polynom $v_1(x) = D(g_1(x),\, g_1'(x))$, který je prvním faktorem polynomu $f(x)$ a je zastoupen v polynomu $f(x)$ první mocninou.

```
In[6]:= v1 = PolynomialGCD[g1, h1 - D[g1, x]]

Out[6]= 5 + x
```

Algoritmus samozřejmě bude ještě dále pokračovat, protože platí $h_1(x) - g_1'(x) \neq 0$. Další postup bude opět analogický, proto netřeba dalších komentářů.

```
In[7]:= g2 = Simplify[g1/v1]

Out[7]= -252 + 300 x - x^2 - 49 x^3 + x^4 + x^5

In[8]:= h2 = Simplify[(h1 - D[g1, x])/v1]

Out[8]= 1020 - 14 x - 549 x^2 + 8 x^3 + 15 x^4

In[9]:= v2 = PolynomialGCD[g2, h2 - D[g2, x]]

Out[9]= -6 + x

In[10]:= g3 = Simplify[g2/v2]

Out[10]= 42 - 43 x - 7 x^2 + 7 x^3 + x^4
```

```
In[11]:= h3 = Simplify[(h2 - D[g2, x])/v2]
Out[11]= 2 (-60 - 9 x + 32 x^2 + 5 x^3)

In[12]:= v3 = PolynomialGCD[g3, h3 - D[g3, x]]
Out[12]= 7 + x

In[13]:= g4 = Simplify[g3/v3]
Out[13]= 6 - 7 x + x^3

In[14]:= h4 = Simplify[(h3 - D[g3, x])/v3]
Out[14]= -11 + x + 6 x^2

In[15]:= v4 = PolynomialGCD[g4, h4 - D[g4, x]]
Out[15]= -1 + x

In[16]:= g5 = Simplify[g4/v4]
Out[16]= -6 + x + x^2

In[17]:= h5 = Simplify[(h4 - D[g4, x])/v4]
Out[17]= 4 + 3 x

In[18]:= v5 = PolynomialGCD[g5, h5 - D[g5, x]]
Out[18]= 3 + x

In[19]:= g6 = Simplify[g5/v5]
Out[19]= -2 + x

In[20]:= h6 = Simplify[(h5 - D[g5, x])/v5]
Out[20]= 1

In[21]:= v6 = PolynomialGCD[g6, h6 - D[g6, x]]
Out[21]= -2 + x
```

Zde algoritmus končí, protože $h_6(x) - g_6'(x) = 0$

```
In[22]:= h6 - D[g6, x]
Out[22]= 0
```

Dále tedy můžeme zobrazit podobu polynomu $f(x)$ po faktorizaci.

```
In[23]:= v1 * v2 ^ 2 * v3 ^ 3 * v4 ^ 4 * v5 ^ 5 * v6 ^ 6

Out[23]= (-6 + x)^2 (-2 + x)^6 (-1 + x)^4 (3 + x)^5 (5 + x) (7 + x)^3
```

Závěrem je opět možné provést zkoušku, zda jsme provedli faktorizaci správně.

```
In[24]:= Expand[%]

Out[24]= 960 180 480 - 4 837 480 704 x + 9 203 362 560 x^2 - 6 897 073 536 x^3 -
         1 161 139 104 x^4 + 4 847 439 168 x^5 - 1 738 450 416 x^6 -
         1 118 110 120 x^7 + 774 661 937 x^8 + 105 626 333 x^9 - 154 605 506 x^10 -
         796 202 x^11 + 18 192 715 x^12 - 542 745 x^13 - 1 348 380 x^14 +
         23 100 x^15 + 60 791 x^16 + 1115 x^17 - 1426 x^18 - 74 x^19 + 13 x^20 + x^21
```

Závěr

V této práci jsme si ukázali přehled některých algoritmů pro rozklad polynomů. Začali jsme od těch nejjednodušších, které jsme dokázali určit bez náročnosti, zda je mnohočlen ireducibilní. Poté jsme přešli ke složitějším, které bylo i více efektivní. Algoritmy vždy dovedly rozklad mnohočlenu vypočítat a došli jsme k závěru, že rozklad polynomu existoval.

Zabývali jsme se také rozkladem polynomu čtvrtého stupně, který je velmi náročný. Předpočítačové éře tato metoda „ručně“ zabrala dost času, oproti dnešní době, kdy za nás náročné výpočty vyřeší výpočetní technika a počítačové programy algebry.

Kroneckerův algoritmus je velmi zdlouhavý, a jeho postup je nepraktický, i když vedl vždy k rozkladu polynomů. Pokud bychom daný polynom nemohli rozložit, pak můžeme při tomto algoritmu konstatovat, že polynom je ireducibilní.

Square-free je dalším algoritmem pro rozklad polynomu v součin faktorů nedělitelných čtvercem. Tento rozklad je jednodušší, než pomocí Kroneckerova algoritmu a je zároveň i rychlejší. K tomuto rozkladu nám postačily znalosti určení formálních derivací a zjištění největších společných dělitelů. Programu *Wolfram Mathematica*® jsme využili k určení největších společných dělitelů polynomů. Ty bychom ani nemohli počítat „ručně“, povšimli jsme si, jak velký kus práce bere při jejich určování „na sebe“ pokročilý software. Nicméně s touto pomocí bylo možné projít i složitou cestu popsanou v algoritmech pro „square-free factorization“.

Resumé

This thesis treats an irreducubility of the polynomials in $\mathbb{Z}[x]$. It is possible to decide an irreducibility of the polynomials using Eisenstein´s criterion. The term of the irreducible polynomial is connected closely with the reducible polynomial in $\mathbb{Z}[x]$. The factorizing of the polynomials into factors is interesting especially for the polynomials with the higher degree than the degree three. Several algorithms exist for this factorizing like Kronecker´s one and algorithms for square – free factorization. Examples and illustrations in program *Wolfram Mathematica* 8® are added to the whole thesis. This advanced software is able to determinate greatest common divisors, which man even cannot to do a calculation.

Seznam použité literatury a internetových zdrojů

[1] Bican, L. Algebra I.(skripta MFF UK Praha) Praha, 1982.

[2] Hora, J.: O některých otázkách souvisejících s využíváním programů počítačové algebry ve škole – I. díl, 1. vydání, Pedagogické centrum Plzeň, 1998.

[3] Drábek, J.; Hora, J.: Algebra. Polynomy a rovnice, 1. vydání, ZČU Plzeň, 2001.

[4] Hora, J.: Eisensteinovo kritérium ireducibility, Rozhledy matematicko-fyzikální, ročník 68 (1989-90), č. 10, str. 434-435.

[5] Hora, J.: Kroneckerův algoritmus, Rozhledy matematicko-fyzikální, ročník 69 (1990-91), č. 5, str. 199-202.

[6] BROOKFIELD, G. Faktoring Quartic Polynomials: A Lost Art. Mathematics Magazine Vol. 80, No. 1(Feb., 2007), pp. 67-70.

[7] PROCHÁZKA, L. a kol. Algebra. Praha: Academia, 1990. ISBN 80-200-0301-0.

[8] Davenport, J. H.; Siret, Y.; Tournier, E.: Computer Algebra, London Academic Press, 1988.

[9] Wright, F. J.: Polynomial GCDs and remainder sequences, Mathematics and Algorithms for Computer Algebra, CBPF, 2003

[10] Počítačová Algebra, Algoritmy, Systémy a Aplikace (http://kfe.fjfi.cvut.cz/~liska/poalg/all.html)

[11] Fotografie a životopis Leopolda Kroneckera (http://www-history.mcs.st-andrews.ac.uk/Biographies/Kronecker.html) (http://en.wikipedia.org/wiki/Kronecker)

[12] Fotografie a životopis Gottholda Eisensteina

(http://www-history.mcs.st-and.ac.uk/Biographies/Eisenstein.htm)

(http://en.wikipedia.org/wiki/Gotthold_Eisenstein)

[13] Encyclopaedia Britannica

(http://www.britannica.com)