O FAKTORIZACI POLYNOMŮ S CELOČÍSELNÝMI KOEFICIENTY

JAROSLAV HORA

ABSTRAKT. Článek obsahuje ukázku užití klasického algoritmu pro faktorizaci polynomu s celočíselnými koeficienty, který objevil Theodor von Schubert. Tento algoritmus posléze znovuobjevil L. Kronecker. Algoritmus je ale vhodný jen pro polynomy jedné neurčité a nevelkého stupně. Nakonec je stručně popsán algoritmus pro faktorizaci polynomu s koeficienty v tělese Z_p, p – prvočíslo. K jeho vypracování přispěli dva čeští, resp. slovenští matematici. Tento algoritmus je základem moderních faktorizačních algoritmů.

ÚVOD

Schopnost faktorizovat polynomy s celočíselnými koeficienty je důležitá jak pro profesionální matematiky, tak pro učitele. V posledních desetiletích zde došlo k fascinujícímu pokroku. Můžeme sledovat českou a slovenskou stopu v matematických základech užívaných algoritmů.

1. KLASICKÝ ALGORITMUS VYUŽÍVAJÍCÍ DĚLITELNOSTI

Stručně naznačme ideu faktorizačního algoritmu, jehož autorem byl astronom Theodor von Schubert (1793). Algoritmus znovuobjevil L. Kronecker. Algoritmus by byl vhodný i pro talentované středoškolské studenty či další zájemce o matematiku.

Příklad: Rozložme polynom $f(x) = x^5 + x^4 + x^2 + x + 2$!

Hledáme faktor $g(x) \in Z[x]$ takový, že $g(x)|f(x)$. Můžeme předpokládat, že st $g(x) \leq 2$. Kvadratický polynom $g(x)$ je určen hodnotami ve třech bodech, kupř. volme $x = 0, 1, 2$. Přitom musí funkční hodnota $g(0)$ dělit $f(0)$, $g(1)$ dělit $f(1)$, $g(2)$ dělit $f(2)$. Vypočtěme nejprve funkční hodnoty $f(0) = 2$, $f(1) = 6$, $f(2) = 56$ a vytvořme množiny $D_{f(0)} = \{1, -1, 2, -2\}$, $D_{f(1)} = \{1, -1, 2, -2, 3, -3, 6, -6\}$, $D_{f(2)} = \{1, -1, 2, -2, 4, -4, 7, -7, 8, -8, 14, -14, 28, -28, 56, -56\}$.

Nyní máme pro výběr $g(0) \in D_{f(0)}$ čtyři možnosti, pro $g(1)$ osm a $g(2)$ šestnáct. V nejhorším případě tedy bude nutné nalézt $4 \cdot 8 \cdot 16 = 512$ interpolačních polynomů $g(x)$ a vždy testovat, zda $g(x)|f(x)$ v $Z[x]$. Pokud to nastane, nalezneme rozklad $f(x) = g(x).\ h(x)$, v opačném případě je $f(x)$ ireducibilní.

I. Kupř. pro trojici $g(0) = 2$, $g(1) = 2$, $g(2) =$ dostaneme interpolační polynom $g(x) = 2$, který zjevně není dělitelem $f(x)$.

II. Pro $g(0) = g(1) = g(2)) = -1$ máme ovšem $g(x) = -1$. Ještě jednou si povšimněme, že interpolační polynom nemusí mít právě stupeň právě 2, ale může mít i stupeň nižší (v daném případě jde dokonce o konstantu). V této ukázce jsme ovšem nalezli triviální dělitel $g(x) = -1$ polynomu $f(x)$, takže je nutné v testování pokračovat. Nyní se pro středoškolské studenty nabízí např. možnost seznámení s Lagrangeovými interpolačními polynomy a jednoduchou metodou jejich výpočtu (viz [5]). Ušetříme čtenáři příp. řadu neúspěšných pokusů a přejdeme rovnou k trojici hodnot vedoucí k řešení.

Received by the editors 10.02.2020
2010 *Mathematics Subject Classification.* 13P05
Key words and phrases. Polynomy s celočíselnými koeficienty, faktorizace, algoritmy pro faktorizaci.

III. Pro trojici $g(0) = 1$, $g(1) = 3$, $g(2) = 7$ dostaneme $g(x) = x^2 + x + 1$, tento polynom dělí $f(x)$ a přivádí nás k rozkladu $f(x) = (x^2 + x + 1)(x^3 - x + 2)$.

Je patrné, jak bychom zapsali algoritmus pro obecný případ, kdy stupeň polynomu $f(x) \in Z[x]$ je n a kdy pro stupeň s eventuálního dělitele $g(x) \in Z[x]$ platí $s \leq \left[\frac{n}{2}\right]$, kde symbol $\left[\frac{n}{2}\right]$ značí tzv. celou část čísla $\frac{n}{2}$. Zásadní nevýhodou popsaného algoritmu však je, že v obecném případě s rostoucím stupněm polynomu $f(x)$ bude exponenciálně růst i počet $s + 1$- tic, které bude nutné probrat a tím i nároky na paměť a na dobu potřebnou k výpočtu. Bude-li tedy stupeň polynomu f větší, nebude algoritmus použitelný.

2. POLYNOMY DĚLITELNÉ ČTVERCEM

Nyní bude možná dobré si připomenout situaci, kdy jsme integrovali tzv. racionální lomené funkce, tj. funkce ve tvaru podílu dvou polynomů s koeficienty z tělesa racionálních či reálných čísel. Podstatným krokem bylo provedení rozkladu jmenovatele v součin lineárních a nerozložitelných kvadratických faktorů, přičemž ale bylo možné, že se v rozkladu tyto faktory vyskytnou i ve vyšší mocnině než první.

Definice: Nechť I je obor integrity s jednoznačným rozkladem a $v(x) \in I[x]$ nechť je polynom. Řekneme, že v**(x) není dělitelný čtvercem**, jestliže neexistuje polynom $u(x) \in I[x]$ kladného stupně takový, že $u^2(x) | v(x)$.

Dále, buď $f(x) \in I[x]$ primitivní polynom, tj. polynom, ze kterého nelze vytknout konstantu větší než 1. Řekneme, že polynom $f(x)$ je rozložen v součin faktorů nedělitelných čtvercem (square–free decomposition), jestliže jej lze psát ve tvaru $f(x) = v_1^1(x)v_2^2(x) \dots v_k^k(x)$, kde žádný z faktorů $v_i(x)$, $i = 1, 2, \dots, k$ není dělitelný čtvercem a výrazy v_i, $i = 1, 2, \dots, k$ jsou po dvou nesoudělné (tj. $D(v_i, v_j) = 1$ pro všechna $i, j = 1, 2, \dots, k$, kde $i \neq j$).

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

Tím se otevírá cesta k postupnému nacházení výrazů v_i, $i = 1, 2, \dots, k$ za předpokladu, že námi užívaný programový balík obsahuje povel pro výpočet největšího společného dělitele dvou polynomů. Programy jako Maple či Mathematica toto splňují, někdejší Derive nikoli. V dalším se tedy můžeme věnovat jen algoritmům pro faktorizaci polynomů nedělitelných čtvercem.

3. FAKTORIZACE POLYNOMŮ MODULO P, P PRVOČÍSLO

Co kdybychom ale studovali faktorizaci polynomů nikoli v $Z[x]$, ale v $Z_p[x]$, tj. nad konečnými p – prvkovými tělesy, kde p je prvočíslo? Zde je zřejmě počet případných faktorů velmi omezen a výhodou může být i známá skutečnost, že $(Z_p[x], +, \cdot)$ je eukleidovský obor integrity.

Příklad: Rozhodněme o reducibilitě či ireducibilitě polynomu $f(x) \in Z[x]$, $f(x) = x^5 - 5x^4 + 7x^3 + 3x^2 - 12x + 15$.

Řešení: Nejprve nalezněme obraz $\overline{f(x)}$ polynomu $f(x)$ při kanonickém homomorfismu φ: $Z[x] \to Z_2[x]$, tj. v zobrazení, při němž jsou původní koeficienty polynomu $f(x)$ nahrazeny nejmenšími nezápornými zbytky při dělení dvěma. Dostaneme $\overline{f(x)} = x^5 + x^4 + x^3 + x^2 + 1$. Kdyby tento polynom byl reducibilní v $Z_2[x]$, musel by být dělitelný buďto lineárním nebo kvadratickým faktorem. Lineárními polynomy x, resp. $x + 1$ však $\overline{f(x)}$ zjevně dělitelný není. Zbývá otestovat dělitelnost ireducibilními kvadratickými faktory. Snadno se zjistí, že v $Z_2[x]$ existuje jediný ireducibilní polynom druhého stupně, a to $x^2 + x + 1$ a tím $\overline{f(x)}$ rovněž není dělitelný.

Kdyby původní polynom $f(x) \in Z[x]$ byl naopak rozložitelný v $Z[x]$, $f(x) = g(x).h(x)$, st $g \geq 1$, st $h \geq 1$, pak ale zřejmě musí platit $\overline{f(x)} = \overline{g(x)} \cdot \overline{h(x)}$ v $Z_2[x]$, st $\overline{g(x)} \geq 1$, st $\overline{h(x)} \geq 1$. Posledně zapsaný rozklad však neexistuje, proto ani $f(x)$ není rozložitelný v $Z[x]$.

Je ovšem třeba mít na paměti, že výpočty v $(Z_p, +, .)$ jsou specifické: kupř. pro každé $a \in Z_p$ je $a^p = a$, (malá věta Fermatova), resp. platí $(a + b)^p = a^p + b^p$. Pro faktorizaci polynomů v $Z_p[x]$ je k dispozici tzv. Berlekampův algoritmus. Uveďme jeho základy a jednu ukázku – detailnější zdůvodnění je dostupné v připojené literatuře.

Vstup: polynom $f(x) \in Z_p[x]$, který není dělitelný čtvercem žádného polynomu ze $Z_p[x]$.

1. Vypočítej matici Q.

2. Najdi bázi jejích vlastních vektorů pro vlastní hodnotu 1. Počet vektorů této báze určuje zároveň počet ireducibilních faktorů polynomu $f(x)$.

3. Vypočti $D(f(x), v(x) - r)$ pro každý prvek $r \in Z_p$, kde $v(x)$ je polynom odpovídající netriviálnímu vlastnímu vektoru. To by mělo poskytnout rozklad polynomu $f(x)$. Je –li nalezeno méně faktorů než očekáváme, je nutno užít jiný vlastní vektor.

Příklad: Nalezněme rozklad polynomu $f(x) = x^4 + x + 1 \in Z_5[x]$.

Řešení:

1. Určení matice Q: Pro $i = 0$ dostáváme kongruenci $x^0 \equiv 1 \bmod f(x)$, 1. řádek matice Q je 1, 0, 0, 0. Pro $i = 1$ dostáváme kongruenci $x^5 \equiv 4x^2 + 4x \bmod f(x)$, tedy druhý řádek matice Q je 0, 4, 4, 0. Dále pro $i = 2$ máme $x^{10} \equiv 2x^3 + x^2 + 4x + 4 \bmod f(x)$ a získáváme třetí řádek matice, a to 4, 4, 1, 2. Pro $i = 3$ nakonec zjistíme, že $x^{15} \equiv 4x^2 + x + 3 \bmod f(x)$, takže čtvrtý řádek matice Q je 3, 1, 4, 0 a $Q = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 4 & 4 & 0 \\ 4 & 4 & 1 & 2 \\ 3 & 1 & 4 & 0 \end{pmatrix}$.

2. Vlastní vektory pro $\lambda = 1$ budou mít tvar (a, b, c, d), $a, b, c, d \in Z_5$.

Je $(a, b, c, d).Q = (a + 4c + 3d, 4b + 4c + d, 4b + c + 4d, 2c) = (a, b, c, d)$. Porovnáním odpovídajících složek vektorů obdržíme rovnice $4c + 3d = 0$, $3b + 4c + d = 0$, $4b + 4d = 0$, $2c = d$. Třetí z těchto rovnic ještě zjednodušme na $b + d = 0$. Volíme –li $c = v$ jako parametr, je $d = 2v$, $b = 3v$, $v \in Z_5$, zatímco a je zřejmě libovolné. Nyní již snadno nahlédneme, že vektorový prostor W lze zapsat pomocí parametrů $u, v \in Z_5$ ve tvaru $W = \{(u, 3v, v, 2v)\}$. Volíme –li kupř. $u = 0$, $v = 1$, resp. $u = 1$, $v = 1$, pak získáme jednu bázi tohoto vektorového prostoru, a to $B = \{(0, 3, 1, 2), (1, 3, 1, 2)\}$. To znamená, že polynom $f(x) \in Z_5[x]$ lze rozložit v součin dvou ireducibilních faktorů.

3. Vezmeme –li vektor (0, 3, 1, 2), je $v(x) = 2x^3 + x^2 + 3x$ a podle shora uvedeného algoritmu dostaneme

pro $r = 0$ $D(x^4 + x + 1, 2x^3 + x^2 + 3x) = 1$,
pro $r = 1$ $D(x^4 + x + 1, 2x^3 + x^2 + 3x + 4) = 1$,
pro $r = 2$ $D(x^4 + x + 1, 2x^3 + x^2 + 3x + 3) = x + 2$,
pro $r = 3$ $D(x^4 + x + 1, 2x^3 + x^2 + 3x + 2) = 1$,
pro $r = 4$ $D(x^4 + x + 1, 2x^3 + x^2 + 3x + 1) = x^3 + 3x^2 + 4x + 3$,

takže jsme nalezli **rozklad $f(x) = x^4 + x + 1 = (x + 2)(x^3 + 3x^2 + 4x + 3)$** v $Z_5[x]$.

Berlekampův algoritmus je součástí velkých programových balíků jako Maple či Mathematica. Algoritmus je pojmenován po Elwynu Ralfu Berlekampovi, který jej popsal ve dvou svých článcích z let 1967 a 1970. Podstatnou roli při budování teoretického základu tohoto algoritmu ale měli K. Petr (1868 – 1950) a Š. Schwarz (1914 – 1996).

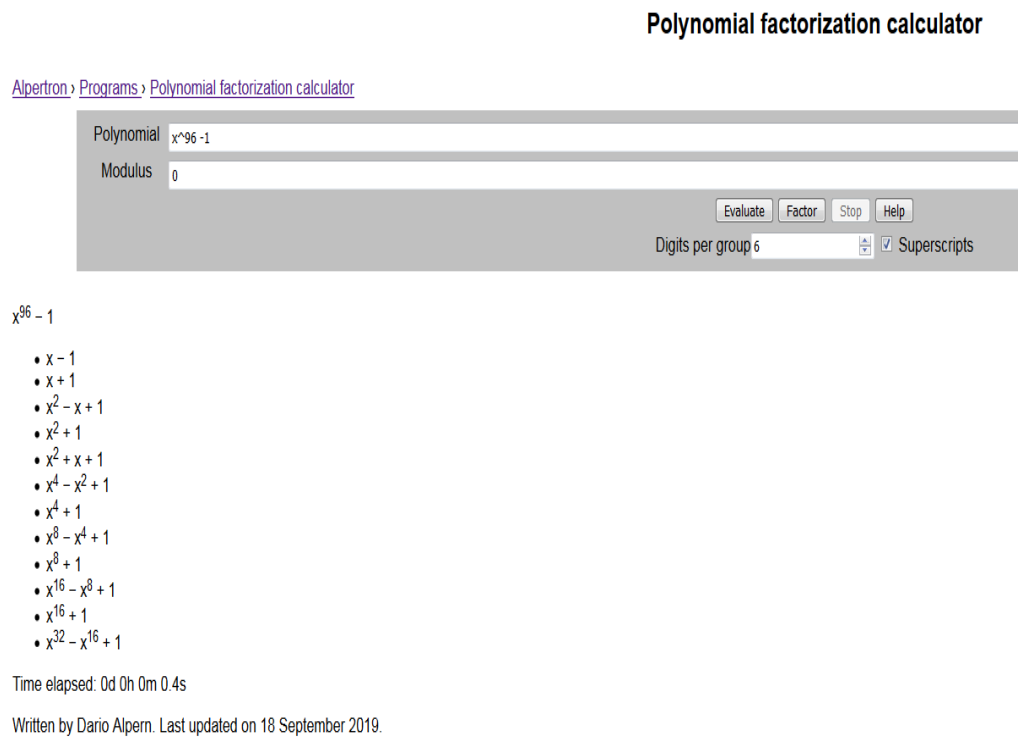
V Petrově práci z r. 1937 jsou počítány řádkové vektory matice Q, avšak nehovoří se zde ještě o matici, nýbrž o lineární substituci. Počítá se zde ale charakteristický polynom matice $Q - I$. Ve fundamentální práci věnované počítačové algebře [2] se Q nazývá Petrova –Berlekampova matice. V sérii článků Š. Schwarze se pak matice Q užívá explicitně.

Závěrem je ještě třeba říci, že ze znalosti faktorizace v $Z_p[x]$ je možné nalézt faktorizaci původního polynomu $f(x) \in Z[x]$. Odpovídající metoda se nazývá Henselovo zdvižení (Hensel's lifting). Kurt Wilhelm Sebastian Hensel v r. 1918 v článku *Eine neue Theorie der*

algebraischen Zahlen (Mathematische Zeitschrift 2, 433 – 452) zavedl p – adická čísla. Jeho metodu (Henselovo zdvižení) využil pro účely počítačové algebry Hans Zassenhaus v r. 1969. Metoda samotná ale byla známa opět již K. F. Gaussovi – viz [3]. V poslední době se k nalezení faktorů v $Z[x]$ užívá takzvaný LLL algoritmus.

Opusťme ale teorii a podívejme se na úžasné výsledky, které dnes můžeme najít např. na mobilu po zadání Calculators + Dario Alpern. Zde je umístěno několik kalkulátorů poskytujících výsledky zejména z oblasti teorie čísel. Pod číslem 10 se nachází Polynomial factorization calculator a v něm si můžeme zadat polynom a to, zda budeme faktorizovat polynomy s celočíselnými koeficienty či v Z_p, p prvočíslo:

3.1. Co dnes můžeme najít na mobilu



OBRÁZEK 1: Faktorizace polynomu na mobilu

LITERATURA

[1] Davenport, J. H., Siret, Y., Tournier, E.: *Computer Algebra*, London, Academic Press, 1988, ISBN 0-12-204230-1.

[2] von zurGathen, J., Gerhard, J.: *Modern Computer Algebra*, Cambridge Univ. Press, 1999, ISBN 0 521 64176 4.

[3] Gauss, C. F.: *Disquisitiones generales de congruentiis. Analysis residuorum caput octavum.* In Werke II, Handschriftlicher Nachlass, ed. R. Dedekind, 212–242. Königliche Gesellschaft der Wissenschaften, Göttingen. Reprinted by Georg Olms Verlag, Hildsheim New York, 1973.

[4] Geddes, K.O., Czapor, S. R., Labahn, G.: *Algorithms for Computer Algebra*, Kluwer Academic Publishers Boston / Dordrecht / London, 1992, ISBN 0-7923-9259-0.

[5] Hora, J.: *Kroneckerův algoritmus*. Rozhledy matematicko–fyzikální, roč. 69, (1990–91), č. 5, str. 199–202.
[6] Hungerford, T. W.: *Algebra*, Springer Verlag, 5. vydání, 1989, ISBN 0-15-543468-3.
[7] Childs, L. N.: A Concrete Introduction to Higher Algebra, Springer, 1979, ISBN 0-387-94484-2.
[8] Lidl, R., Niederreiter, H.: *Introduction to finite fields and their applications*, Cambridge Univ. Press, revised edition, Cambridge 1994, ISBN 0 521 46094 8.
[9] Petr, K.: Über die Reduzibilität eines Polynoms mit ganzzahligen Koeffizienten nach einem Primzahlmodul. Časopis pro pěstování matematiky a fyziky 66, (1937), 85–94.
[10] Procházka, L. a kol.: Algebra, Academia, Praha, 1990.
[11] Schwarz, Š.: *Sur le nombre des racines et des facteurs iréducibiles d' une congruence donné*. Časopis pro pěstování matematiky a fyziky 69, (1940), 128 –145.
[12] Schwarz, Š.: *Contribution a la réductibilité des polynômes dans la théorie des congruences.* Věstník Královské české společnosti nauk, Třída matematicko - přírodovědná, 1939, Praha, 1 – 7.
[13] Schwarz, Š.: *On the reducibility of polynomials over a finite field*. Quarterly Journal of Mathematics Oxford 7 (2) (1956), 110 – 124.
[14] Schwarz, Š.: *Об одном классе многочленов над конечным телом*. Matematicko-fyzikálny časopis 10 (1960) , 68 – 80.
[15] Schwarz, Š.: *О числе неприводимых факторов данного многочлена над конечным полем*. Czechoslovak Mathematical Journal 11 (86) (1961) , 213 – 225.
[16] Waerden, B. L. van der: *Algebra I, II*, Berlin – Göttingen – Heidelberg, Springer Verlag 1960. Ruský překlad, *Algebra*, Nauka, Moskva, 1976.

KMT FPE ZČU PLZEŇ, ČESKÁ REPUBLIKA
E-mail address : horajar@kmt.zcu.cz