život se zabýval středoškolským matematickým vzděláváním. V této oblasti publikoval více než 200 článků a na konci života mu byly vydány dvě na sebe navazující knižní monografie.

Stanislav Trávníček zesnul 2. 6. 2017. Pro každého z nás zůstane vzorem po stránce odborné a pedagogické, zejména však ale po stránce lidské. Čest jeho památce!

Redakce časopisu Matematika–fyzika–informatika

Kroneckerův algoritmus

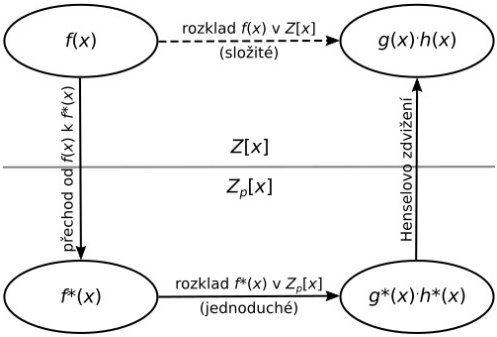
LUKÁŠ HONZÍK

Fakulta pedagogická ZČU v Plzni

V současné době si již většina matematiků a učitelů matematiky neumí představit život bez využívání systémů počítačové algebry. Poměrně známý je v tomto směru například program Wolfram Mathematica, který zvládá řešit široké spektrum nejen matematických problémů. Mimo jiné dovede celkem rychle provádět i faktorizaci polynomů v $Z[x]$, kterou je na základních a hlavně středních a vysokých školách často nutné zvládnout. Do programu stačí zadat příslušný příkaz a mnohočlen, který chceme rozložit, řekněme kupříkladu $x^{95} - 5x^{70} - 12x^{65} - 4x^{53} + x^{50} + 3x^{45} + 60x^{40} + + 20x^{28} - 5x^{25} - 36x^{15} - 12x^3 + 3$, a během okamžiku je proveden rozklad a na obrazovku se vypíše výsledek $(x^{45} - 12x^{15} - 4x^3 + 1) \cdot (x^{50} - 5x^{25} + 3)$. Rychlost a efektivnost zmíněného procesu je zajištěna skutečností, že program disponuje sofistikovanými algoritmy pro výpočet faktorů – například algoritmy pro faktorizaci polynomů v končených tělesech prostřednictvím Petrovy–Berlekampovy matice (připomeňme, že za poznatky v této oblasti stojí nemalý příspěvek československých matematiků Karla Petra a Štefana Schwarze) a Henselovým zdvižením. Schéma takto pojaté faktorizace je znázorněno na obr. 1.

Počátky systému Mathematica a jemu podobných programů však byly o poznání skromnější. Zároveň je také nutné připomenout, že i některé v dnešní době relativně často používané programy – například známý program Derive, případně různé volně šiřitelné aplikace pro tablety a chytré telefony – si stále musí vystačit s jednoduššími metodami. Ty je sice ome-

zují při zpracovávání složitějších úloh, avšak pro běžnou práci jsou stále dobře použitelné. Zároveň takto jde ukázat lidskou vynalézavost a důvtip, které dovolily tyto matematické problémy řešit dávno před tím, než se vůbec objevily první počítače, na nichž by takovéto postupy mohly být aplikovány v podobě nám dnes známé jako počítačové algoritmy. Jedním z takových starších postupů v případě faktorizace polynomů s celočíselnými koeficienty je tzv. *Kroneckerův algoritmus*.



Obr. 1

Leopold Kronecker a historie

Kroneckerův algoritmus nese jméno významného pruského matematika Leopolda Kroneckera (1823 až 1891). Základy jeho matematického vzdělání položili soukromí učitelé najímaní Kroneckerovými rodiči a dále byly prohloubeny na gymnáziu, kde jej vyučoval matematik Ernst Eduard Kummer. Ten také rozpoznal Kroneckerův talent a všemožně jej podporoval. Při studiích na Berlínské univerzitě se sice Kronecker nevěnoval jen studiu matematiky, zajímaly jej také chemie, astronomie či meteorologie, jeho doktorská práce pak již ale byla zaměřena matematicky a týkala se algebraické teorie čísel. Po skončení studií se roce 1861 stal členem Berlínské akademie věd, byl editorem v Crellově matematickém časopise a v roce 1884 byl jmenován členem Královské společnosti v Londýně.

Zajímavostí pro čtenáře budiž skutečnost, že přestože algoritmus nese Kroneckerovo jméno, nebyl tím, kdo jej vymyslel. Tato zásluha patří Hermannu Schubertovi, dalšímu německému matematikovi, který ideu algoritmu pro faktorizaci polynomů popsal již v poslední dekádě 18. století. Kronecker pak po více než půlstoletí Schubertův algoritmus znovuobjevil a upravil pro širší použití.

Základní myšlenka algoritmu

Samotný algoritmus sloužící k nalezení rozkladu polynomu $f(x)$ v $Z[x]$ v součin dvou polynomů $g(x)$ a $h(x)$ nižších stupňů je vcelku jednoduchou záležitostí a skládá se z 5 kroků:

1) Hledáme jistý mnohočlen $g(x)$ s celočíselnými koeficienty stupně $\mathrm{st}(g) \geq 1$, který dělí zadaný mnohočlen $f(x)$ v $Z[x]$, jehož stupeň je $\mathrm{st}(f) = n$. Omezíme se pouze na ty polynomy, jejichž stupeň je rovný hodnotě $s = [n/2]$ (celá část zlomku), anebo menší než tato hodnota. Jedná se tedy o horní odhad stupně hledaného polynomu $g(x)$ vycházející z faktu, že pro tři polynomy $f(x)$, $g(x)$ a $h(x)$, kde $f(x) = g(x) \cdot h(x)$, platí rovnost $\mathrm{st}(f) = \mathrm{st}(g) + \mathrm{st}(h)$. Bez újmy na obecnosti jde tedy předpokládat, že $\mathrm{st}(g) \leq \mathrm{st}(h)$; pokud by tomu tak nebylo, provedli bychom přeznačení obou polynomů. Mezní případ nastane při rovnosti $\mathrm{st}(g) = \mathrm{st}(h)$, kdy lze psát $\mathrm{st}(f) = 2\,\mathrm{st}(g)$. Proto je nutné hledat stupeň polynomu $g(x)$ v intervalu $1 \leq \mathrm{st}(g) \leq s$, kde $\mathrm{st}(g) \in Z$.

2) Dosazením $s + 1$ hodnot, například $x = 0, 1, \ldots, s$, do předpisu $f(x)$ dostaneme $s + 1$ celočíselných funkčních hodnot.

3) Dělí-li hledaný mnohočlen $g(x)$ zadaný polynom $f(x)$, musí nutně i jeho funkční hodnoty v bodech $x = 0, 1, \ldots, s$ dělit příslušné funkční hodnoty polynomu $f(x)$. Tedy platí $g(0)|f(0), g(1)|f(1), \ldots, g(s)|f(s)$, a proto zavedeme množiny $D_{f(0)}$, $D_{f(1)}$, $\ldots$, $D_{f(s)}$ dělitelů čísel $f(0)$, $f(1)$, $\ldots$, $f(s)$. Pokud by pro některou z hodnot $f(i)$, $i = 0, 1, \ldots, s$, platilo $f(i) = 0$, znamená to, že jsme pouhým dosazením zjistili jeden kořen mnohočlenu $f(x)$. Polynom $g(x)$ bychom pak mohli psát jako $g(x) = x - i$ a pro rozklad polynomu $f(x)$ by platila rovnost $f(x) = (x - i) \cdot h(x)$, přičemž $h(x) \in Z[x]$ a $\mathrm{st}(h) = \mathrm{st}(f) - 1$. Pokud naopak pro žádnou hodnotu $f(i)$, $i = 0, 1, \ldots, s$, neplatí $f(i) = 0$, jsou všechny množiny $D_{f(0)}$, $D_{f(1)}$, $\ldots$, $D_{f(s)}$ konečné.

4) Za pomoci vybraných $s + 1$ hodnot $g(0) \in D_{f(0)}$, $g(1) \in D_{f(1)}$, $\ldots$, $g(s) \in D_{f(s)}$ vypočteme polynom $g(x)$, který v bodě $x = 0$ nabývá hodnoty $g(0)$, v bodě $x = 1$ hodnoty $g(1)$ atd.

   Určení tohoto polynomu provedeme užitím postupu pro nalezení Newtonova interpolačního polynomu při znalosti výše vybraných $s + 1$ funkčních hodnot. Jeho zápis je ve tvaru

$$g(x) = \lambda_0 + \lambda_1(x - x_0) + \lambda_2(x - x_0)(x - x_1) + \ldots + \lambda_s(x - x_0) \cdots (x - x_{s-1}),$$

přičemž dopočtení koeficientů $\lambda_0, \lambda_1, \ldots, \lambda_s$ lze zjednodušit zápisem do tzv. „schématu rozdílů“

$$
\begin{array}{ccccccc}
g(x0) & & & & & & \\
& \Delta g(x_0) & & & & & \\
g(x_1) & & \Delta^2 g(x_0) & & & & \\
& \Delta g(x_1) & & \Delta^3 g(x_0) & & & \\
g(x_2) & & \Delta^2 g(x_1) & & & \ldots & \\
& \Delta g(x_2) & & & \ldots & & \\
g(x_3) & & \ldots & & & & \\
& \ldots & & & & & \\
\ldots & & & & & , &
\end{array}
$$

kde $\Delta g(x_i) = g(x_{i+1}) - g(x_i)$, $\Delta^2 g(x_i) = \Delta g(x_{i+1}) - \Delta g(x_i)$, atd., a následným dosazením zjištěných hodnot do vzorce

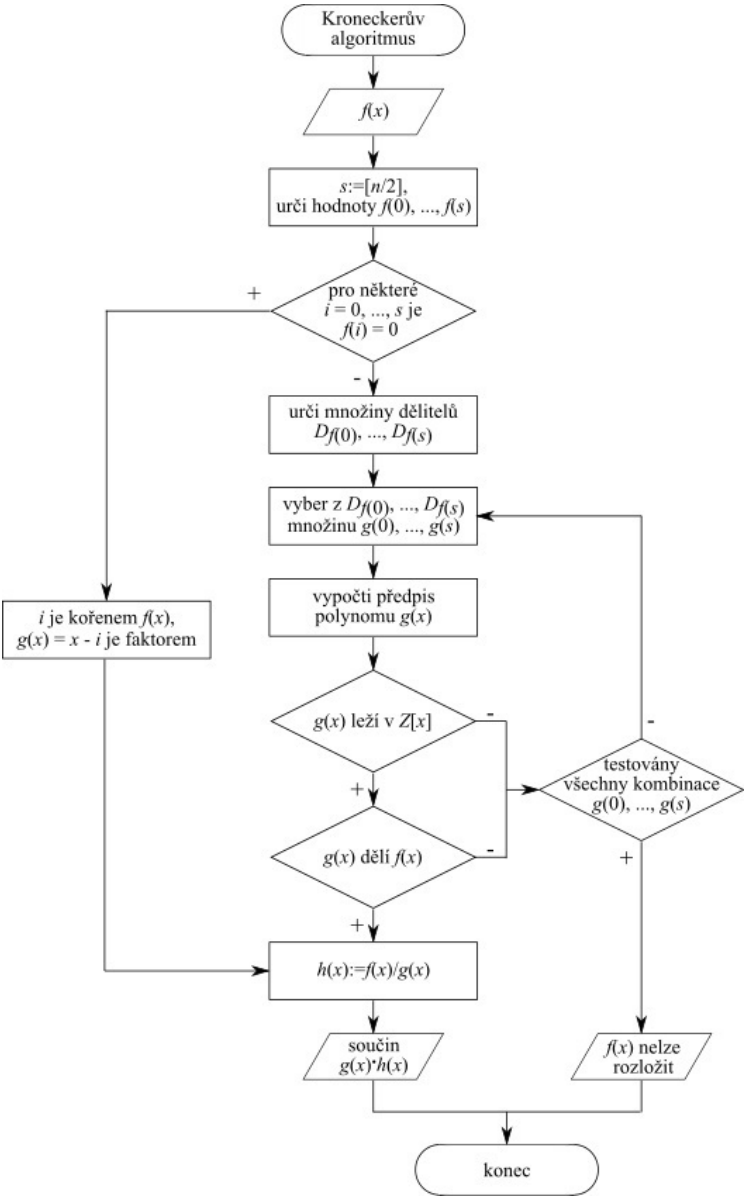
$$\lambda_k = \frac{\Delta^k g(x_i)}{k!}.$$

5) Takto získaný polynom $g(x)$ nemusí nutně být mnohočlenem s celočíselnými koeficienty, v takovém případě je třeba se vrátit ke kroku 4) a vybrat jinou množinu $s+1$ hodnot $g(0), g(1), \ldots, g(s)$.

   Patří-li naopak $g(x)$ mezi polynomy s celočíselnými koeficienty, musíme otestovat, zda je faktorem mnohočlenu $f(x)$, čili zda v $Z[x]$ dělí tento mnohočlen. Pokud platí $g(x)|f(x)$, nalezli jsme faktor polynomu $f(x)$ a můžeme psát $f(x) = g(x) \cdot h(x)$, kde $g(x), h(x) \in Z[x]$, $\mathrm{st}(g) > 0$, $\mathrm{st}(h) > 0$. Pokud naopak $g(x)$ nedělí $f(x)$, je třeba vrátit se ke kroku 4) a vybrat jinou množinu $s+1$ hodnot $g(0), g(1), \ldots, g(s)$.

   Vyzkoušíme-li touto cestou všechny možné kombinace $s+1$ hodnot z množin $D_{f(0)}$, $D_{f(1)}$, …, $D_{f(s)}$ a přesto nenalezneme žádný odpovídající faktor $g(x)$, je zřejmé, že polynom $f(x)$ je nerozložitelný.

Celý algoritmus pak můžeme jednodušeji znázornit pomocí vývojového diagramu (obr. 2). Pro úplnost ještě předveďme praktické použití na několika vybraných úlohách.


Kroneckerův algoritmus
f(x)
s:=[n/2], urči hodnoty f(0), ..., f(s)
pro některé i = 0, ..., s je f(i) = 0
+
-
urči množiny dělitelů Df(0), ..., Df(s)
vyber z Df(0), ..., Df(s) množinu g(0), ..., g(s)
vypočti předpis polynomu g(x)
i je kořenem f(x), g(x) = x - i je faktorem
g(x) leží v Z[x]
-
+
testovány všechny kombinace g(0), ..., g(s)
-
g(x) dělí f(x)
-
+
+
h(x):=f(x)/g(x)
součin g(x)·h(x)
f(x) nelze rozložit
konec

Obr. 2

Ilustrační příklady

Úloha 1

Nalezněte v $Z[x]$ rozklad polynomu $f(x) = x^3 + x^2 + x + 1$.

Řešení. Stupeň polynomu $f(x)$ je $\mathrm{st}(f) = 3$, hledaný mnohočlen $g(x)$ tedy musí být maximálně prvního stupně, neboť $s = [3/2] = 1$, a pro výpočet tak potřebujeme dvě funkční hodnoty $f(x)$. Volme $x \in \{0, 1\}$, čímž získáváme $f(0) = 1$ a $f(1) = 4$. Žádná z funkčních hodnot není nulová, a tak vytvoříme množiny dělitelů $D_{f(0)} = \{\pm 1\}$, $D_{f(1)} = \{\pm 1, \pm 2, \pm 4\}$. V nejhorším případě by tedy bylo nutné otestovat 12 různých kombinací. Pro první pokus vyberme například kombinaci hodnot $g(0) = 1$ a $g(1) = 1$, schéma rozdílů pak vypadá následovně:

$$\begin{array}{cc} 1 & \\ & 0 \\ 1 & \end{array}$$

Poté dostáváme koeficienty $\lambda_0 = \frac{1}{0!} = 1$ a $\lambda_1 = \frac{0}{1!} = 0$, takže polynom $g(x)$ by měl být ve tvaru $g(x) = \lambda_0 + \lambda_1(x - 0) = 1 + 0(x - 0) = 1$. Je zřejmé, že nalezený polynom $g(x) = 1$ je sice ze $Z[x]$, ale zároveň je konstantní, přičemž z libovolného polynomu jde vždy vytknout hodnotu 1, která nás v tuto chvíli nezajímá. Je tedy nutné zvolit jinou kombinaci prvků z množin dělitelů.

Vyberme $g(0) = 1$ a $g(1) = 4$, poté schéma rozdílů vypadá takto:

$$\begin{array}{cc} 1 & \\ & 3 \\ 4 & \end{array}$$

a koeficienty mají hodnoty $\lambda_0 = \frac{1}{0!} = 1$ a $\lambda_1 = \frac{3}{1!} = 3$. Po dosazení do vzorce dostáváme $g(x) = 1 + 3(x - 0) = 3x + 1$. Tento polynom je sice ze $Z[x]$ a dokonce prvního stupně, ale pokud bychom se jím pokusili vydělit zadaný mnohočlen $f(x)$, podílem by již nebyl polynom s celočíselnými koeficienty. Proto je nutné otestovat jinou kombinaci z množin dělitelů.

Zvolme $g(0) = 1$ a $g(1) = 2$, potom dostaneme schéma rozdílů ve tvaru:

$$\begin{array}{cc} 1 & \\ & 1 \\ 2 & \end{array}$$

a koeficienty mají hodnoty $\lambda_0 = \frac{1}{0!} = 1$ a $\lambda_1 = \frac{1}{1!} = 1$. Dostáváme polynom $g(x) = 1 + 1(x - 0) = x + 1$, který patří do $Z[x]$ a zároveň dělí polynom

$f(x)$. Podíl je $f(x) : g(x) = x^2 + 1$ a můžeme psát výsledný rozklad

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

Úloha 2

Nalezněte v $Z[x]$ rozklad polynomu $f(x) = x^5 + 3x^4 + 2x^3 + 2x^2 + 1$.

Řešení. Stupeň polynomu $f(x)$ je $\mathrm{st}(f) = 5$, stupeň hledaného polynomu $g(x)$ tedy musí být maximálně $\mathrm{st}(g) = [5/2] = 2$. Pro jeho výpočet budeme potřebovat 3 funkční hodnoty $f(x)$: $f(0) = 1$, $f(1) = 9$ a $f(2) = 105$. Utvoříme množiny dělitelů, kde $D_{f(0)} = \{\pm 1\}$, $D_{f(1)} = \{\pm 1, \pm 3, \pm 9\}$ a $D_{f(2)} = \{\pm 1, \pm 3, \pm 5, \pm 7, \pm 15, \pm 21, \pm 35, \pm 105\}$. V nejhorším případě bychom nyní potřebovali vyzkoušet $2 \cdot 6 \cdot 16$ možných kombinací, abychom mohli konstatovat, že polynom $f(x)$ je ireducibilní.

Vyberme následující trojici $g(0) = 1$, $g(1) = 3$ a $g(2) = 7$ a ve schématu rozdílů obdržíme

$$\begin{array}{ccccc} 1 & & & & \\ & 2 & & & \\ 3 & & & 2 & \\ & 4 & & & \\ 7 & & & & \end{array}$$

takže koeficienty budou $\lambda_0 = \frac{1}{0!} = 1$, $\lambda_1 = \frac{2}{1!} = 2$, $\lambda_2 = \frac{2}{2!} = 1$. Po dosazení dostaneme $g(x) = 1 + 2(x - 0) + 2(x - 0)(x - 1)$, což se po roznásobení rovná $g(x) = x^2 + x + 1$. Tento mnohočlen v $Z[x]$ beze zbytku dělí polynom $f(x)$, je tedy jeho faktorem a můžeme psát jeho rozklad ve tvaru

$$f(x) = (x^2 + x + 1)(x^3 + 2x^2 - x + 1).$$

Nakonec řešme ještě jeden ilustrační příklad, na kterém ukážeme, že Kroneckerův algoritmus není právě efektivním prostředkem faktorizace.

Úloha 3

Rozhodněte v $Z[x]$, zda je polynom $f(x) = x^{10} - 2x^9 + 5x^8 - 4x^7 + 4x^6 + + x^4 - 2x^3 + 5x^2 - 4x + 4$ rozložitelný.

Řešení. Zadaný polynom je stupně $\mathrm{st}(f) = 10$, proto hledaný faktor $g(x)$ bude mít stupeň maximálně $\mathrm{st}(g) = 5$. Pro jeho vypočtení potřebujeme 6 funkčních hodnot, což je poměrně velké množství. Algoritmus v tuto chvíli můžeme zefektivnit vhodnou volbou hodnot nezávisle proměnných x takových, že získané funkční hodnoty budou mít „malé“ množství dělitelů. Nejvhodnější se jeví hodnoty $f(-2) = 4\,160$, $f(-1) = 32$, $f(0) = 4$,

$f(1) = 8$, $f(2) = 1\,040$, $f(3) = 46\,720$, jelikož ostatní funkční hodnoty jsou již příliš velké.

Pokud nyní vytvoříme množiny dělitelů zmíněných funkčních hodnot, zjistíme, že množiny $D_{f(-2)}$, $D_{f(-1)}$, $D_{f(0)}$, $D_{f(1)}$, $D_{f(2)}$ a $D_{f(3)}$ obsahují postupně 56, 12, 6, 8, 40 a dokonce 64 dělitelů. To dohromady činí 82 575 360 možných kombinací eventuálních funkčních hodnot hledaného mnohočlenu $g(x)$. V tuto chvíli je zřejmé, jak časově a paměťově náročný takovýto výpočet rozkladu polynomu může být. Pokud by bylo nutné projít všechny zmíněné kombinace, abychom mohli konstatovat ireducibilitu zadaného polynomu, a věnoval-li by počítač každé z těchto kombinací pouhých 10 milisekund, zabral by celý proces celkem více než 229 hodin, tedy více než 9,5 dne.

Pro pořádek poznamenejme, že zadaný polynom $f(x)$ v $Z[x]$ rozložitelný je, hledání faktorů by tedy nedosahovalo takových velkých časových nároků, a úplný rozklad lze zapsat jako součin $(x^2+1)(x^2-x+2)^2(x^4-x^2+1)$.

Závěr

Jak jsme ukázali v poslední úloze, nemusí být rozkládaný polynom nikterak vysokého stupně a i při nejlepší snaze o optimalizaci může být nakonec celý proces nadmíru výpočetně náročný. Kvůli tomu je Kroneckerův algoritmus i přes poměrně elegantní a jednoduchou základní myšlenku v řadě případů nepoužitelný a v dnešní době jsou v systémech počítačové algebry dostupné sofistikovanější výpočetní postupy, jak bylo zmíněno na začátku textu. I tak se ale jedná o část matematické historie a pěkný důkaz lidské vynalézavosti a důvtipu, který může být výhodně použit například jako dobrá motivace nadaných žáků a studentů k dalšímu a hlubšímu studiu matematiky a výpočetní techniky.

Literatura

[1] *von Gathen, J. – Gerhard, J.*: Modern Computer Algebra. 2nd ed., Cambridge University Press, Cambridge, 2003.

[2] *Hora, J.*: Kroneckerův algoritmus. Rozhledy matematicko-fyzikální, roč. 69 (1990), č. 5, s. 199–202.

[3] MacTutor History of Mathematics [online]. University of St. Andrews, St. Andrews, 2016 [cit. 2017-01-31]. Dostupné z: http://www-history.mcs.st-and.ac.uk/