Po stopách Eukleidova algoritmu HMI

Alena Šolcová
Katedra aplikované matematiky
FIT ČVUT v Praze

Evropský sociální fond
Investujeme do vaší budoucnosti

2014 - 2020

EA - prototyp algoritmického postupu

Eukleidův algoritmus je pro matematiky tradičně prototyp algoritmického postupu.

Objevuje se nejen při hledání NSD (GCD), ale take při řešení neurčitých rovnic (Bézoutova identita), také ve Sturmově metodě při hledání počtu reálných kořenů algebraických rovnic.

Nejstarší použití EA

- Explicitní vyjádření algoritmu před Eukleidem dosud nebylo nenalezeno.
- Aristarchos ze Samu

  O velikostech a vzdálenostech Slunce a Měsíce

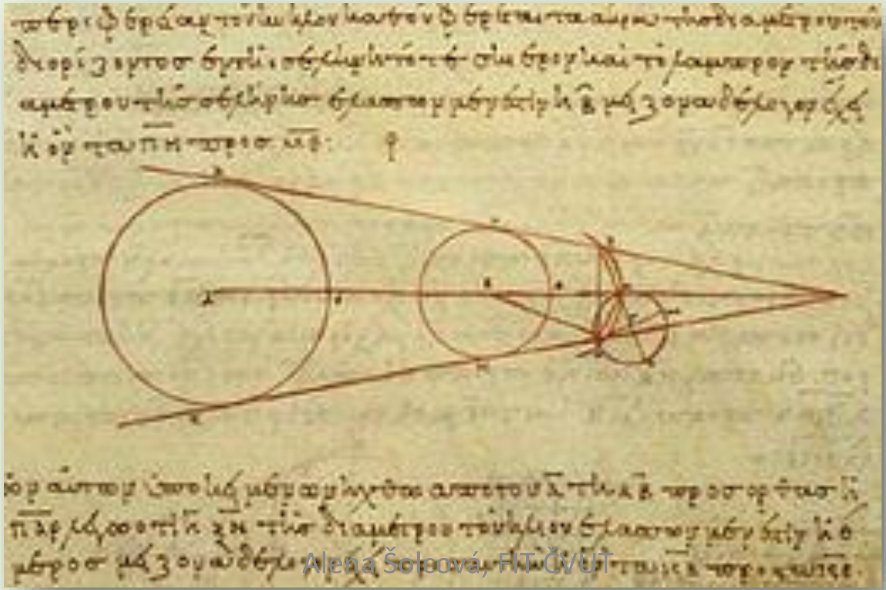
  Aristarchos použil EA dvakrát
  a uvádí poměry, které nahradil jinými podle EA.
- Později Archimédés

  EA používá konkrétně ve 3 aproximacích.
- EA souvisí také s metodou anthyphairesis,

  kterou již užívali v Platónově Akademii.

Aristarchos (310 – 230 př. n. l.)

- žák Stratóna z Lampsaku,
- ovlivněn pýthagorejcem Philoláem z Krotónu,
- citován Archimédem ve spisu *Počítání písku*
- odhad vzdálenosti Měsíce



Aristarchos II

- 71 755 875 : 61 735 500

  → 43 : 37

- 7921 : 4050

  → 88 : 45

Rekonstrukce Aristarchova postupu

- Nechť A = 71 755 875   B = 61 735 500

A – B   = C … … 10 020 375

B – 6C = D … …   1 613 250

C – 6D = 340 875

____

C = 6D, B = 6C + D = 37D

A = B + C = 43 D, tedy A : B = 43 : 37

Rekonstrukce Aristarchova postupu II

- Teprve v 17. stol. byl tento postup spojen s řetězovými zlomky.
- Pokračujme v předcházejícím příkladu:

D = 1 613 250 a E = 340 875

D – 4E = F … 249 750

E – F = G … 91 125

F – 2G = H … 67 500

G – H = I … 23 625

H - 2I = J … 20 250

I – J = K … 3 375

J – 6K = 0

NSD (A, B) = K = 3 375

Pocta Aristarchovi

Riccioli , 17. století

Archimédés (287 -212 př. n. l.)

- Archimédés: *Měření kruhu*

  6336 : 2017 + ¼ → 3 + 10/71 (= 223 : 71)

Poměr obvodu kruhu k průměru je

menší než 3 + 1/7 a větší než 3 + 10/71.

$$3 + 1/7 > \pi > 3 + 10/71.$$

Archimédés II

- Vepisuje do kruhu *n*-úhelníky:

6-úhelník	6 . 153/265	< 3,47
12-úhelník	12 . 153/571	< 3,22
24-úhelník	24 . 153/(1161 + 1/8)	< 3,16
48-úhelník	48 . 153/(2334 + ¼)	< 3,147
96-úhelník	96 . 153/(4673 + ½)	< 3 + 1/7

VII. kniha Eukleidových Základů

- Dva výroky o EA lze najít v VII. knize Eukleidových Základů:
- Prop.1: O tom, kdy jsou dvě čísla vzájemně nesoudělná: *Jsou-li dána dvě čísla nestejná a odčítá-li se střídavě vždy menší od většího, když zbývající předcházejícího nikdy nedoměřuje, dokud nezbude jednotka, počáteční čísla budou navzájem kmenná.*
- Prop.2: O určení největšího společného dělitele: *Jsou-li dána dvě čísla navzájem nekmenná, najdi největší jejich společnou míru.* (Překlad Františka Servíta z roku 1907.)
- To je nejdůležitější místo v Základech a odtud EA lze obecně odvodit!

Nový překlad, 2011

- Řecké matematické texty, Oikoymenh, Praha 2011, str. 190-194
- Kniha VII, Prop. 1: *Jsou dána dvě nestejně velká čísla a odebírejme střídavě a opakovaně menší od většího. Pokud nikdy nedojde k tomu, že by zbývajícím číslem bylo měřeno číslo z předchozího kroku, dříve než dospěje k jednotce, pak čísla daná na počátku jsou nesoudělná.*
- Kniha VII, Prop. 2: *Jsou dána dvě čísla, která nejsou nesoudělná, a máme nalézt jejich největší společnou míru.*

Eukleidovy Základy, Kniha X.

- Prop. 2: *Jestliže se ze dvou daných nestejně velkých veličin odebírá střídavě a opakovaně vždy ta menší od té větší, přičemž zbytek nikdy neměří předchozí zbytek, pak jsou tyto veličiny nesouměřitelné.*

ŘMT, str. 214 -215

- Prop. 3:

Jsou-li dány dvě veličiny souměřitelné, najdi jejich míru. Servít, str. 160 - 161

V. kniha Eukleidových Základů

Pak je tu ještě jedna větev,

vycházející z V. knihy Eukleidových Základů.

Prop. 5: ***Když jest veličina veličiny stejným násobkem jako část odečtená odečtené, též zbytek zbytku bude stejným násobkem, jakým čísla celá.***

- Jde zde o porovnávání poměrů,

na to navázal arabský matematik al-Chajjám

(přepis bývá různý, např. al-Khayyam)

a v 9. stol. al-Mahani.

Isa Al-Mahani (820–880),

- Perský matematik a astronom, který v letech 853 - 866 zaznamenal řadu pozorování měsíčních a slunečních zatmění a konjunkce planet.
- Komentoval Eukleidova a Archimédova díla. Zdokonalil překlad Menelaovy Sfériky.
- Pokusil se řešit tzv. Archimédův problém: Rozdělit kouli rovinou na dvě části v daném poměru objemu.

  Řešení vede ke kubické rovnici $x^3 + c^2 . b = c . x^2$

  Muslimští matematici ji nazývají al-Mahaniho rovnicí.

Přesnost Mahaniho výpočtů

- Ibn Yunus:

  „Počítal s astrolábem počátky měsíčních zatmění a po třech po sobě následujících zatměních se zmýlil pouze o hodinu a půl.“

- Al- Mahani napsal také práci,

kde dokazuje 26 problémů sporem.

- Motivaci k zájmu o matematiku

  čerpal převážně z astronomie.

Bézoutova identita

Celočíselné řešení x_0, y_0 lineární rovnice

$$ax - by = c,$$

existuje vždy a splňuje Bézoutovu identitu

$$ax_0 - by_0 = 1.$$

- To ovšem neobjevil Bézout, ale

  Bachet de Méziriac v roce 1624.

Bézout podobné vysvětlení uvádí až ve 3. části svého *Kursu matematiky* v roce 1766.

Étienne Bézout (1730 – 1783)

- Francouzský matematik
- *Théorie générale des équations algébriques*, Paříž 1779, teorie eliminace a symetrických funkcí kořenů rovnic
- Používal determinanty v roce 1764, nevyložil jejich obecnou teorii.

Příklad

- **Cours d' Algebre, 1766**

  Řeší úlohu: $17x - 11y = 542$

$y = (17x - 542)/11 = (17x - 98.11)/11$

$= (17x/11) - 98$

$y = x - 49 + (6x - 3)/11$ a $6x - 3 = 11u$,

hledáme celé číslo x, tedy $x = (11u + 3)/6.$

$x = 39 + 11$

$50 + 11$

$61 + 11$

etc.

$y = 11 + 17$

$28 + 17$

etc.

Bézoutova identita:

$2.17 - 3.11 = 1$

Claude Gaspard Bachet de Méziriac

- 1581 – 1638
- Bachet byl první

  v Evropě, který se zabýval řešením neurčitých rovnic pomocí řetězových zlomků.
- Zabýval se teorií čísel, nalezl např. metodu konstrukce magických čtverců.
- Je považován za autora Bézoutovy identity.

Řetězové zlomky

- **Aristarchos ze Samu**, **Archimédés**,
- **Fibonacci** – aproximace tzv. zlatého řezu

  v *Liber abaci*, 1202,

  Bombelli - aproximace druhé odmocniny

  v jeho spisu *Algebra*, 1572 , **Cataldi** - *Trattato*, 1613.
- Počátek těchto úvah: X. kniha Eukleidových Základů - v pojednání o nesouměřitelných veličinách, v Prop. 2 počátek těchto úvah.

Řetězové zlomky II

- Brahmagupta (598 - 670) byl první, který vyjádřil, že řetězový zlomek není zobrazení – je to *limita* posloupnosti zobrazení.
- Pak se řetězovým zlomkům věnovali již nám známí Arabové - al-Mahani, 9. stol., a al-Chajjam, 12. stol.
- Nakonec přejdeme do Anglie:

lord Brouncker našel formuli pro 4/pi a tuto formuli citoval Wallis ve svém díle *Arithmetica infinitorum.*

Euclid's algorithm, mathematics and music

Benjamin Wardhaugh, Plus Magazine,

Issue 40, September 2006

A little while ago I was reading some letters written by the 17th century German mathematician Gottfried Leibniz to an obscure contemporary of his, **Conrad Henfling**. The letters were about music theory and the details of how to tune musical instruments. I was surprised to find that at one point Henfling started to use Euclid's algorithm to justify his musical reasoning.

- How useful could a mathematical technique from the third century BC be to a 17th-century musician? Very useful indeed, it turns out. Euclid's algorithm provides a way of dealing with equations of musical pitch, potentially helping musicians and instrument makers to tune musical instruments.

Interval hudební a matematický

Interval mezi oktávou a kvintou

poměr $a - n \times b = c$, kde $b > c$

- oktáva - kvinta = kvarta 2:1 / 3:2 = 4:3 (1)
- kvinta - kvarta = tón 3:2 / 4:3 = 9:8 (2)
- kvarta - 2 tóny = půltón
  (např. E k F) $4:3 / (9:8)^2 = 256:243$ (3)
- tón - 2 půltóny = komma

$9:8 / (256:243)^2 = 531441:524288$ (4)

Jaká je vhodná aproximace kvinty v oktávě?

Interval	Poměr
• půltón - 3 kommy = 'X '	$256:243/(531441:524288)^3 = (2^8:3^5) / (3^{12} : 2^{19})^3 = 2^{65} : 3^{41}$
• komma - 'X' = 'Y'	$(3^{12} : 2^{19}) / (2^{65} : 3^{41}) = 3^{53} : 2^{84}$
• 'X' - 5'Y' = 'Z'	$(2^{65} : 3^{41}) / (3^{53} : 2^{84})^5 = 2^{485} : 3^{306}$ (>1}

Jaká je vhodná aproximace kvinty v oktávě?

Mohli bychom pokračovat dále nekonečněkrát (ln 4/3 - irac.).

Předpokládejme, že tón - 2 půltóny = 0

Potom **1 tón = 2 půltóny** (5)

kvarta = 2 tóny + 1 půltón (podle 3) = 5 půltónů (podle 5) (6)

kvinta = kvarta + tón (podle 2) = 7 půltónů (podle 5 a 6) (7)

oktáva = kvinta + kvarta (podle 1) = 12 půltónů (podle 5 a 7) (8)

Tedy Eukleidův algoritmus nám pomůže v tom, že můžeme zdůvodnit, že skutečně používaná aproximace kvinty v oktávě **7/12 je optimální (při zanedbání kommy)**, protože kvinta je přibližně 7 půltónů a oktáva jich má asi 12 .

Další krok

- tón = půltón^2 . komma .... $T = P^2 . K$
- kvarta ... □ □ $= T^2 P = K^2 . P^5$
- kvinta ... Q $Q = □ . T = K^3 . P^7$
- oktáva (diapazon) ... D $D = □ . Q = K^5 . P^{12}$

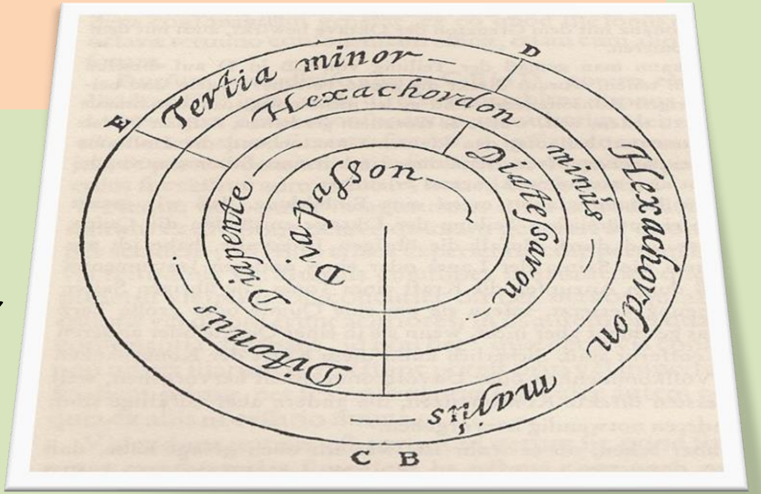
DNES:

- Temperované ladění používá pro půltón 12. odmocninu ze dvou.
- Kvinta pak je $2^{7/12}$ (poměr frekvencí).
- Oktáva je přesná, tj. přesně 2.

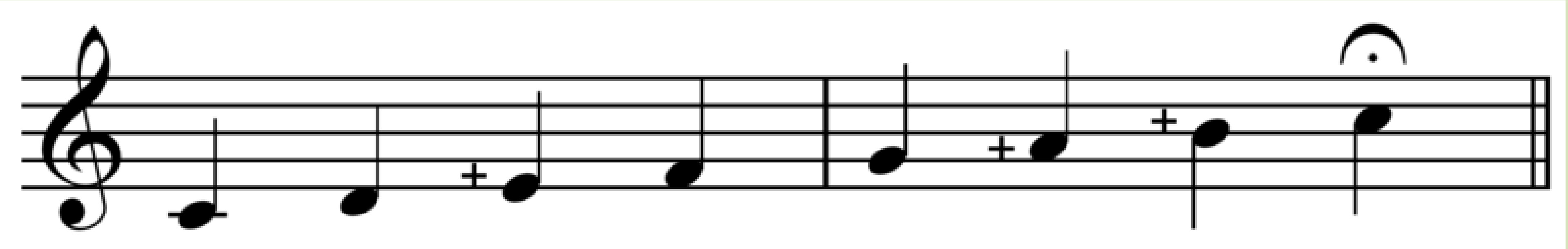
Lord William Brouncker (1620 -1684)

- Irský matematik a hudebník, zakladatel a první president Královské společnosti v Londýně. Loyální royalista. Zabýval se řetězovými zlomky a počítal logaritmy pomocí nekonečných řad. Od 16 let studoval v Oxfordu. Doktorem medicíny (fyziky) se stal v roce 1647.
- Navrhoval tvar lodí, například navrhl tvar jachty pro Karla II. Dopisoval si s Johnem Wallisem.

William Brouncker II



- Brouncker našel obsah části rovnoosé hyperboly pomocí součtu určité řady.
- Přeložil Descartovo *Hudební kompendium*, 1653, a našel nové rozdělení diapasonu na 17 stejných půltónů.



John Wallis (1616 – 1703)

- Anglický matematik, který se podílel na vývoji infinitezimálního počtu.
- Mezi roky 1643 a 1689 pracoval jako kryptograf pro parlament Spojeného králov-ství a později pro královský dvůr.
- Také zavedl symbol ∞ pro nekonečno.

Byla po něm pojmenována planetka 31 982 Johnwallis.

Kryptografie ve Wallisově době

- Kryptografie nebyla v té době na moc dobré úrovni. Navzdory individuálním úspěchům matematiků, mezi které patřil např. François Viète, nebyly principy návrhu a analýzy šifer moc dobře pochopeny.
- Většina cifer závisela na tajném algoritmu namísto proměnlivého klíče.
- Wallis si uvědomil, že druhá možnost je mnohem bezpečnější.

Wallis - kalkulátor

- Studoval v Cambridge.
- Od roku 1649 profesorem geometrie v Oxfordu, předtím určitou dobu knězem.
- Wallisova mimořádná matematická schopnost – počítat zpaměti. Špatně spal, často si počítal a v noci vstával. Jednou v noci spočítal z hlavy druhou odmocninu čísla s 53 ciframi a ráno diktoval výsledek zpaměti – 27-ciferné číslo.

Aplikace řetězových zlomků a EA

- Také Christian Huygens použil řetězové zlomky, kdy počítal počet zubů pro konstrukci planetaria (1682), *De automato planetario.*
- Astronomové vůbec ve svých výpočtech potřebovali často EA.

$$x = b_0 + \cfrac{a_1}{b_1 + \cfrac{a_2}{b_2 + \cfrac{a_3}{b_3 + \cfrac{a_4}{b_4 + \ddots}}}}$$

Christian Huygens (1629 – 1695)

- Huygensův princip
- kyvadlové hodiny
- základy integrálního počtu
- kvadratura kruhu atd.

- Software Huygens
- Sonda Huygens
- Hora na Měsíci, kráter na Marsu, planetka 2801

Model sluneční soustavy

Tehdy byl známý

poměr oběžných dob Saturnu a Země kolem Slunce 29, 43 : 1

Huygens hledal vhodnou aproximaci a

zvolil počet zubů v poměru **206 : 7** = 29, 4285

1. aprox.: 29, 43 ≈ 29 + 1 / (2 + …) = 59/2
2. aprox.: ≈ 29 + 1 / (2 + 1/(3 + …)) = **206/7**
3. aprox.: ≈ 29+1/(2+1/(3+1/14)))=2943/100

18. a 19. století

- Nakonec bychom se mohli věnovat pracem Eulera, Lagrange a Sturma, speciálně čínským matematikům.
- České práce prvního profesora matematiky v češtině **Františka Josefa Studničky** o řetězových zlomcích a teorii čísel jsou přístupné v **České digitální knihovně.**

Leonhard Euler (1707 – 1783)

- analytická teorie řetězových zlomků
- vyjádření transcendentních funkcí
- 1748 **Leonhard Euler,**
  Introductio in analysin infinitorum,
  Vol. I, Chapter 18.
- Otázka konvergence nekonečného řetězového zlomku je analogická
  konstrukci iracionálního čísla jako limity Cauchyho posloupnosti racionálních čísel.

Joseph Louis Lagrange (1736-1813)

- Použil řetězové zlomky k nalezení obecného řešení **Pellovy rovnice**.

$$\boldsymbol{x^2 - n\, y^2 = 1}$$

- Počet kořenů rovnice – otázku formuloval **René Descartes** ve svém díle ***„Géometrie***“, 1637

- **Kaskádová metoda –** Lagrangeův název pro řetězové zlomky

Jacques Charles François Sturm

- 1803 Ženeva – 1855 Paříž
- Vychovatel syna Mme de Stael

  a syna astronoma Araga,
- profesor l’Ecole polytechnique

  a pařížské univerzity.

Sturmova metoda

- $Nx^{m} + Px^{m-1} + Qx^{m-2} + \ldots + Tx + U = 0$

- $V = 0$

  $V = V_1Q_1 - V_2$

  $V_1 = V_2Q_2 - V_3$

  …
- $V_{r-2} = V_{r-1}Q_{r-1} - V_r$

Donald Knuth a 20. století

- Donald Knuth (nar. 10. 1. 1938)

„Počínaje rokem 1950
je slovo
algoritmus
spojeno s ***Eukleidovým algoritmem****.“*

1. díl slavného

The Art of Computer Programming